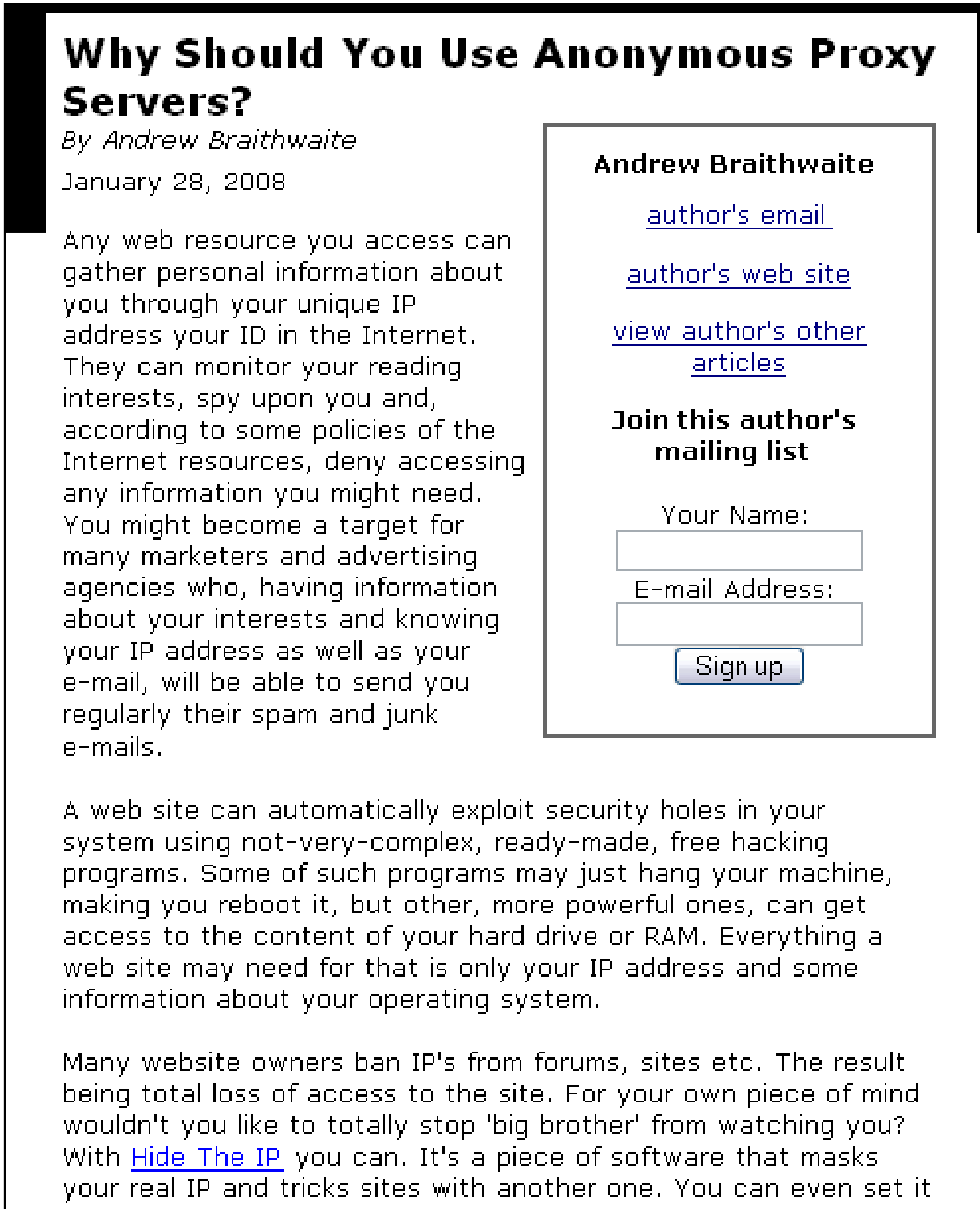
Ethical Hacking and Countermeasures

Version 6

Module LIV

Proxy Server Technologies

News



Why Should You Use Anonymous Proxy Servers?

By Andrew Braithwaite

January 28, 2008

Andrew Braithwaite

author's email

author's web site

view author's other articles

Join this author's mailing list

Your Name:

E-mail Address:

Sign up

Any web resource you access can gather personal information about you through your unique IP address your ID in the Internet. They can monitor your reading interests, spy upon you and, according to some policies of the Internet resources, deny accessing any information you might need. You might become a target for many marketers and advertising agencies who, having information about your interests and knowing your IP address as well as your e-mail, will be able to send you regularly their spam and junk e-mails.

A web site can automatically exploit security holes in your system using not-very-complex, ready-made, free hacking programs. Some of such programs may just hang your machine, making you reboot it, but other, more powerful ones, can get access to the content of your hard drive or RAM. Everything a web site may need for that is only your IP address and some information about your operating system.

Many website owners ban IP's from forums, sites etc. The result being total loss of access to the site. For your own piece of mind wouldn't you like to totally stop 'big brother' from watching you? With Hide The IP you can. It's a piece of software that masks your real IP and tricks sites with another one. You can even set it

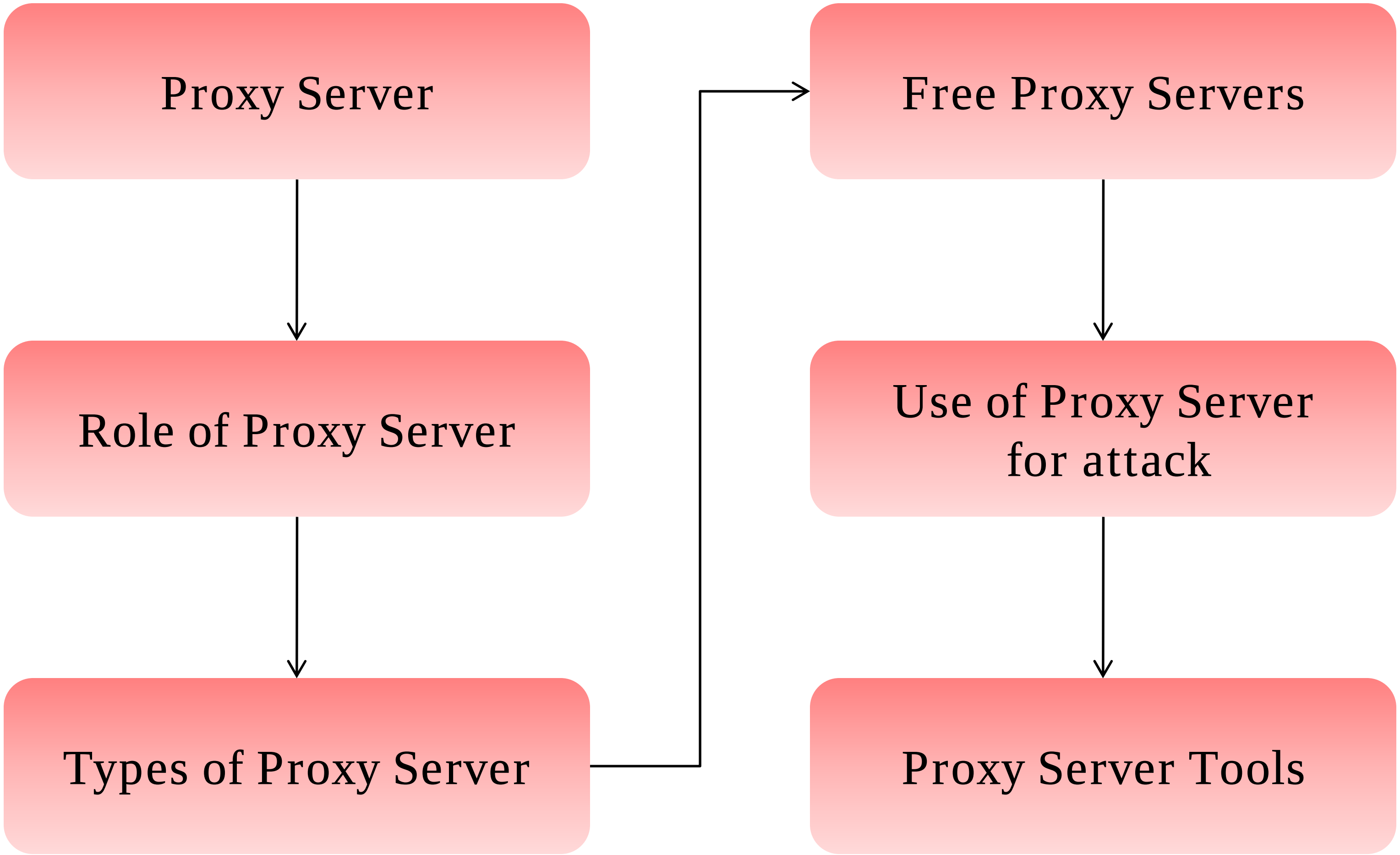
Source: *http://www.americanchronicle.com/*

Module Objective

This module will familiarize you with:

- Proxy server
- Role of proxy server
- Types of proxy server
- Free proxy servers
- Use of proxy server for attack
- Proxy server tools

Module Flow



Proxy Server

Role of Proxy Server

Types of Proxy Server

Free Proxy Servers

Use of Proxy Server for attack

Proxy Server Tools

EC-Council

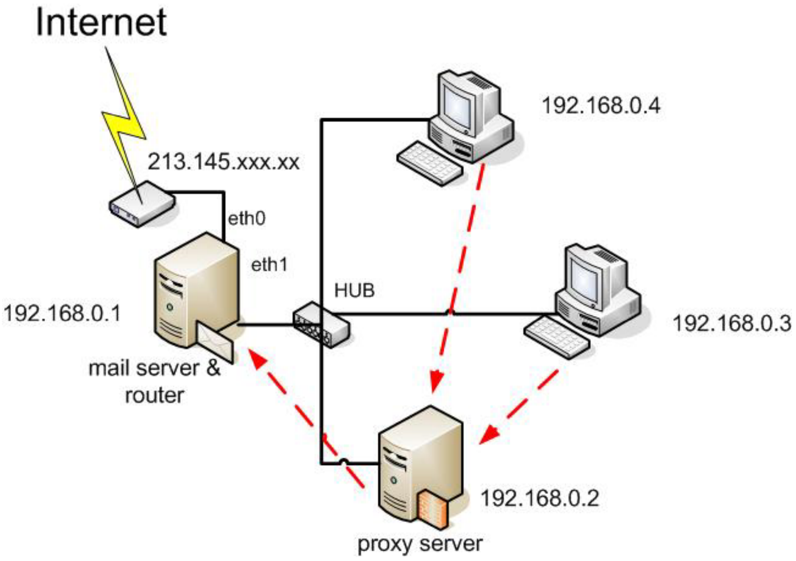
Introduction: Proxy Server

Proxy servers is a server, which acts as an intermediary between internal users and external host

Proxy server protects and hides the computer from the outside network

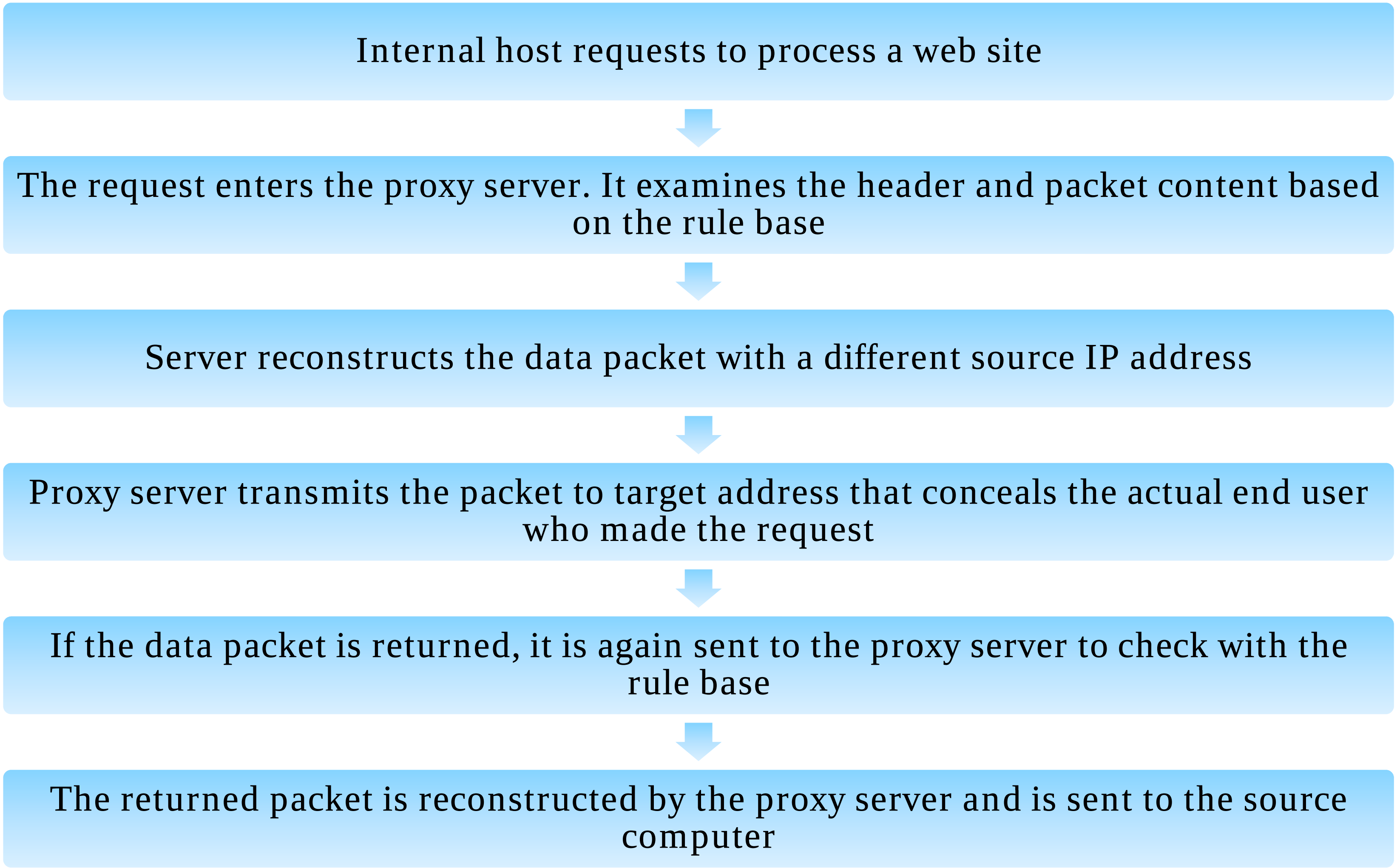
It concentrates on the port that monitors the incoming and outgoing traffic of each port

Proxy server can also be used for the filtering of the request



EC-Council

Working of Proxy Server



Internal host requests to process a web site

The request enters the proxy server. It examines the header and packet content based on the rule base

Server reconstructs the data packet with a different source IP address

Proxy server transmits the packet to target address that conceals the actual end user who made the request

If the data packet is returned, it is again sent to the proxy server to check with the rule base

The returned packet is reconstructed by the proxy server and is sent to the source computer

Types of Proxy Server

Caching Proxy Server

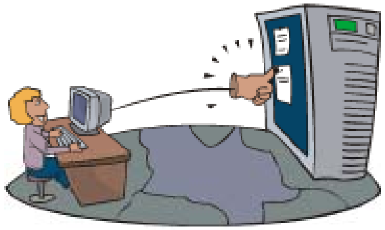
- Caching is servicing the request of clients with the help of saved contents from previous request, without contacting specified server

Web Proxy

- Proxy targeted to the World Wide Web is called Web Proxy
- Web proxy serve as web cache

Anonymizing Proxy Server

- Anonymizing Proxy Server tries to annonimize web surfing



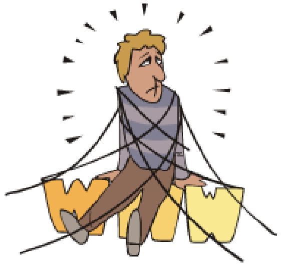
Types of Proxy Server (cont’d)

Hostile Proxy

- It is used to eavesdrop upon the dataflow between the client machine and the web

Intercepting Proxy server

- It combines proxy server with a gateway
- Commonly used in businesses to prevent avoidance of acceptable use policy and ease of administration



Forced Proxy

- Combination of Intercepting and non-intercepting policies

EC-Council

Types of Proxy Server (cont’d)

Open proxy Server

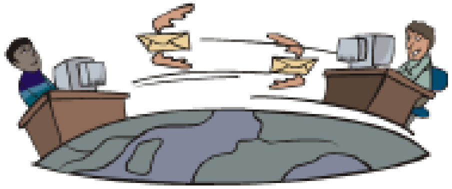
- It is a proxy which can be accessible by any Internet user

Split Proxy Server

- A split proxy is a proxy implemented as two programs installed on two different computers

Reverse Proxy Server

- It is a proxy server that is installed in the neighborhood of one or more web servers
- It validates and processes a transaction in such a way that actual parties do not communicate directly



Types of Proxy Server (cont’d)

Circumventor

- A circumventor is a method of defeating blocking policies which are implemented using proxy servers
- Most circumventors are also proxy servers

Transparent proxy

- It is a proxy that does not modify the request or response beyond what is required for proxy authentication and identification
- It works on the port 80

Non Transparent Proxy

- It is a proxy that modifies the request or response in order to provide some added services to the user agent
- Web requests are directly sent to the proxy regardless of the server from where it originated

Socks Proxy

The socks is an IETF (Internet Engineering Task Force) standard

It is like a proxy system which supports the proxy aware applications

The SOCKS package includes or contains the following components:

- A SOCK server for the specified operating system
- A client program such as FTP, telnet, or the Internet browser
- A client library for the SOCKS

The socks proxy server doesn't allow the external network components to collect the information of the client which had generated the request

Free Proxy Servers

Attacks using thousands of proxy servers around the world are difficult to trace

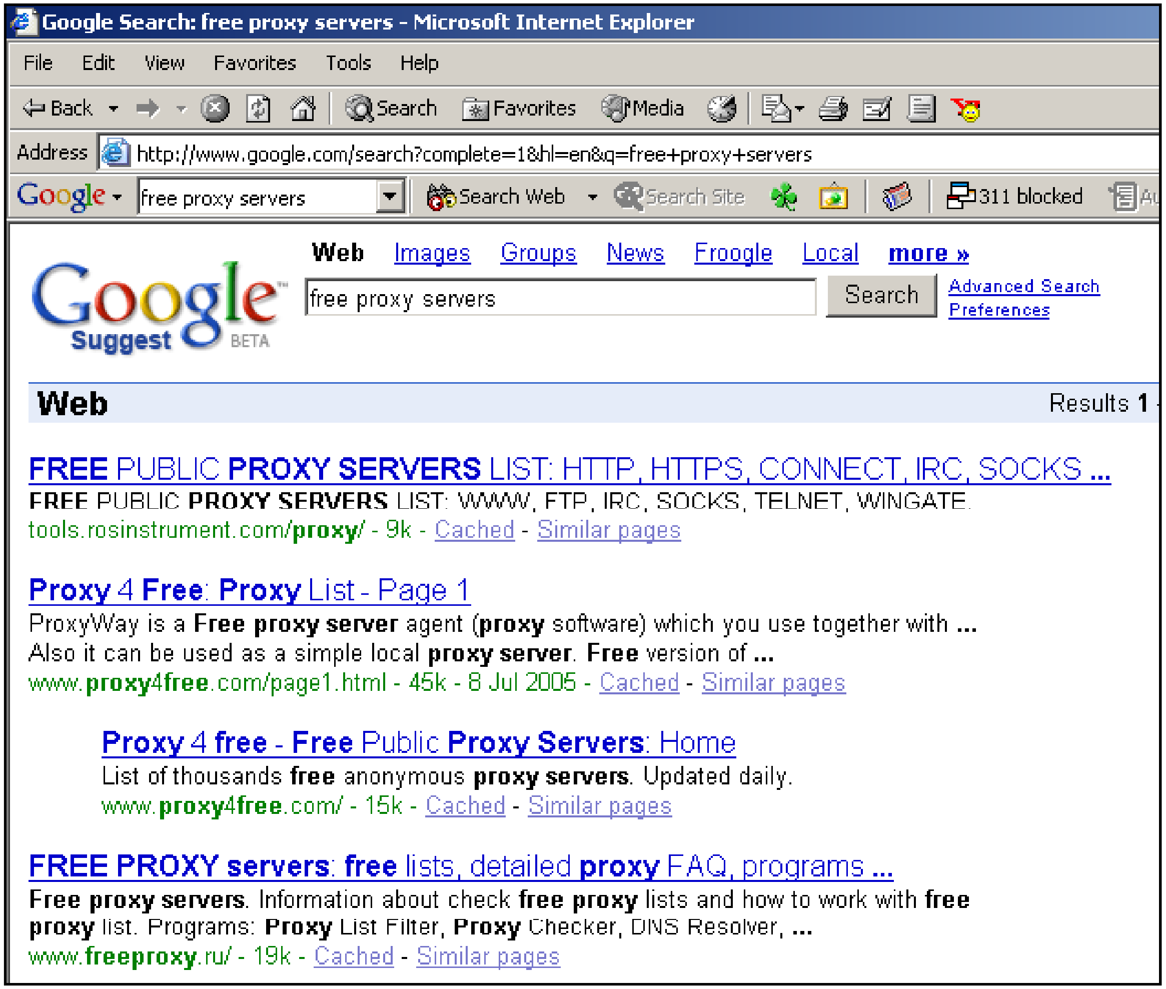
Thousands of free proxy servers are available on the Internet

Search for “free proxy servers” in Google

Some of them might be a honeypot to catch hackers red-handed

Using proxy servers can mask your trace

Free Proxy Servers (cont'd)


Google Search: free proxy servers - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.com/search?complete=1&hl=en&q=free+proxy+servers
Google free proxy servers Search Web Search Site 311 blocked
Web Images Groups News Froogle Local more »
Google Suggest BETA
free proxy servers
Search
Advanced Search
Preferences
Web
Results 1

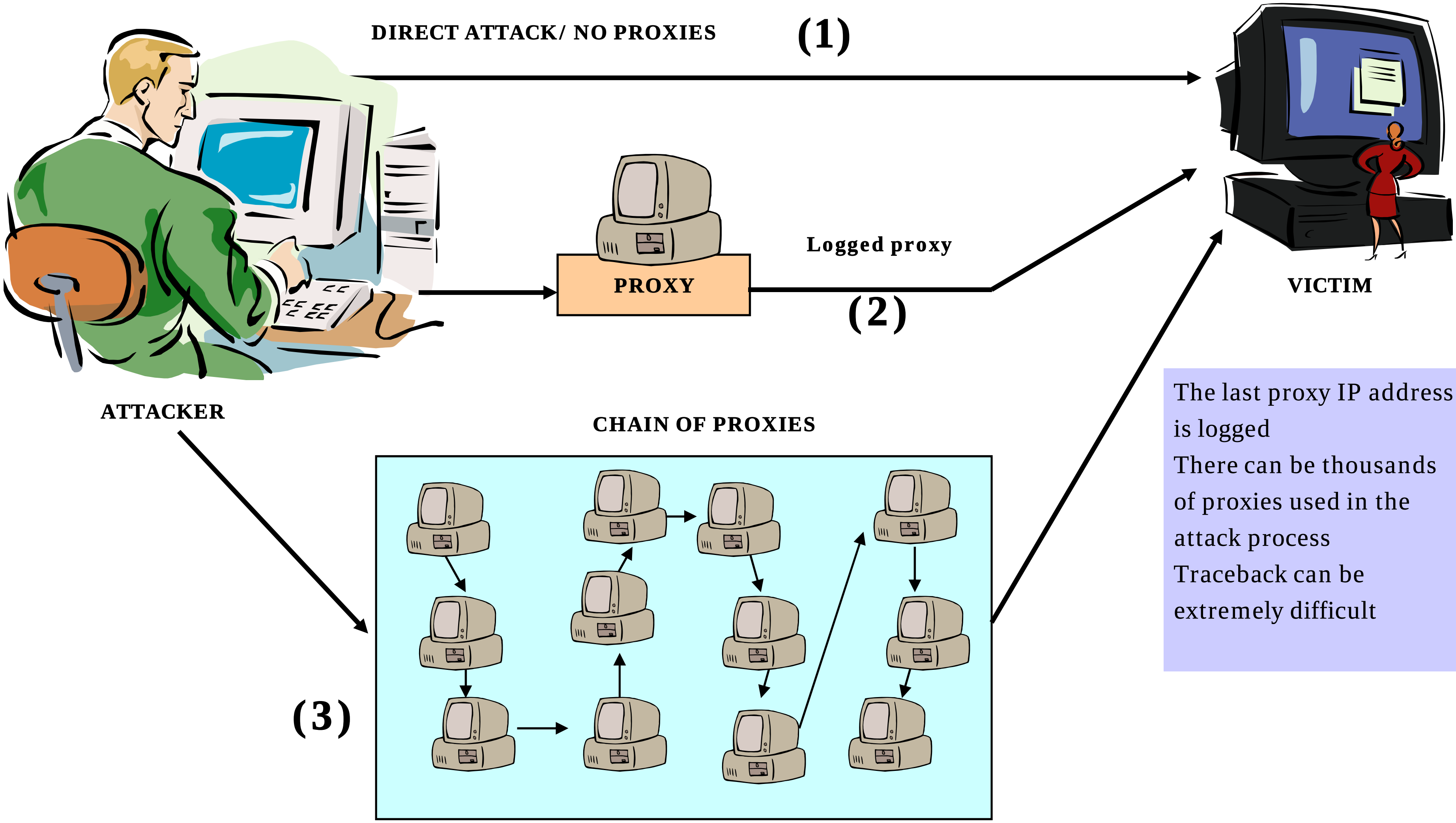
FREE PUBLIC PROXY SERVERS LIST: HTTP, HTTPS, CONNECT, IRC, SOCKS ...
FREE PUBLIC PROXY SERVERS LIST: WWW, FTP, IRC, SOCKS, TELNET, WINGATE.
tools.rosinstrument.com/proxy/ - 9k - Cached - Similar pages

Proxy 4 Free: Proxy List - Page 1
ProxyWay is a Free proxy server agent (proxy software) which you use together with ...
Also it can be used as a simple local proxy server. Free version of ...
www.proxy4free.com/page1.html - 45k - 8 Jul 2005 - Cached - Similar pages

Proxy 4 free - Free Public Proxy Servers: Home
List of thousands free anonymous proxy servers. Updated daily.
www.proxy4free.com/ - 15k - Cached - Similar pages

FREE PROXY servers: free lists, detailed proxy FAQ, programs ...
Free proxy servers. Information about check free proxy lists and how to work with free proxy list. Programs: Proxy List Filter, Proxy Checker, DNS Resolver, ...
www.freeproxy.ru/ - 19k - Cached - Similar pages

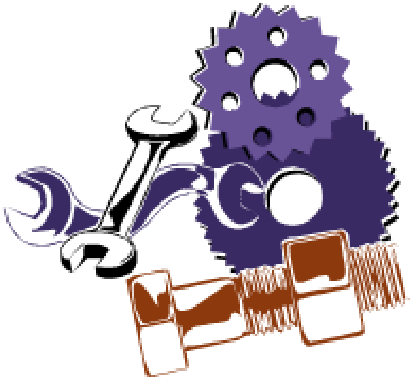
Use of Proxies for Attack



The last proxy IP address is logged

There can be thousands of proxies used in the attack process

Traceback can be extremely difficult



Tools

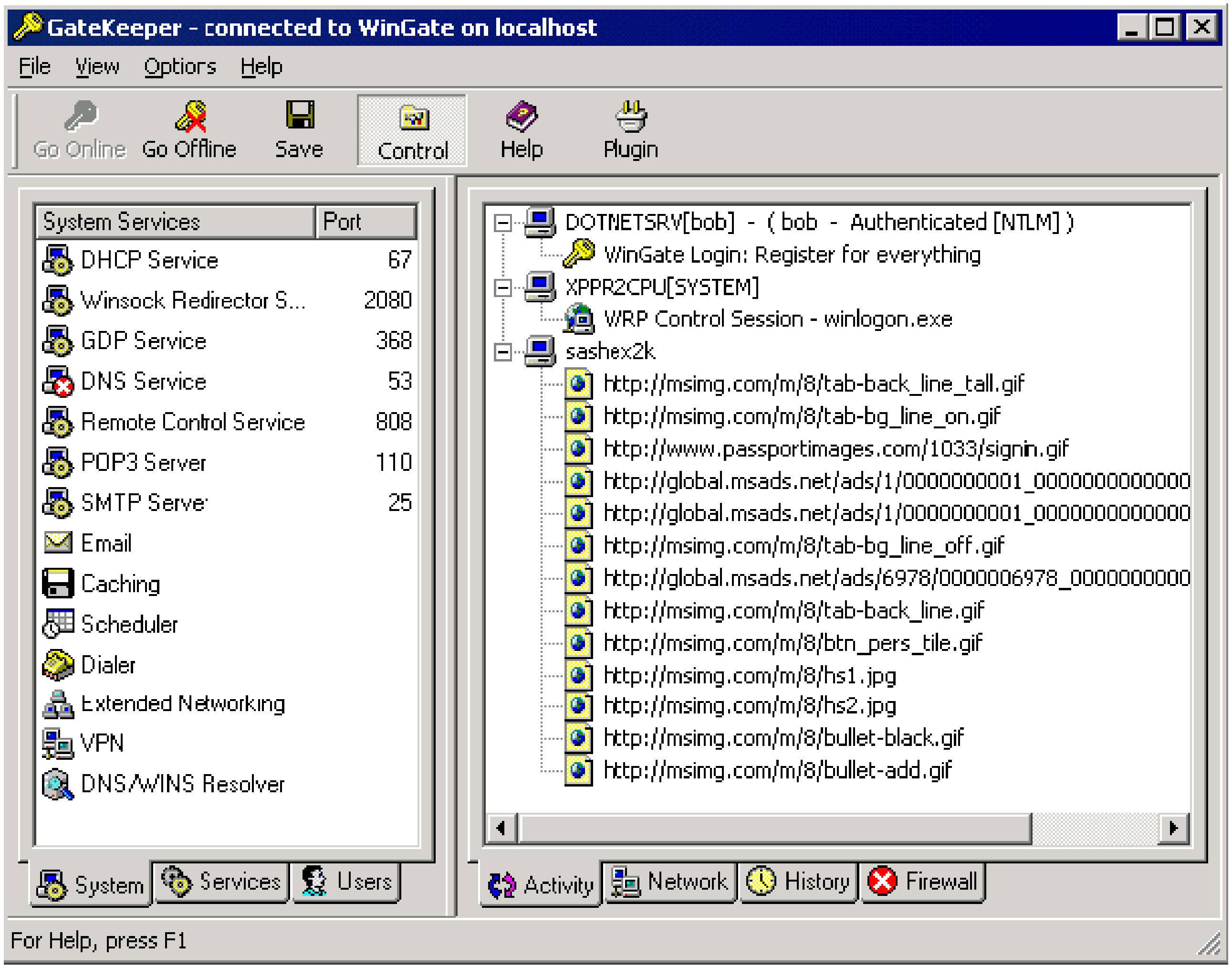
WinGate

WinGate is a sophisticated integrated Internet gateway and communications server designed to meet the control, security, and communications needs

Features:

- Protect servers from internal or external threats
- Enforce advanced and flexible access-control and acceptable use policies
- Improve network performance and responsiveness with web and DNS caching
- Monitor usage in real time, and maintain per-user and per-service audit logs

WinGate: Screenshot



System Services	Port
DHCP Service	67
Winsock Redirector S...	2080
GDP Service	368
DNS Service	53
Remote Control Service	808
POP3 Server	110
SMTP Server	25
Email	
Caching	
Scheduler	
Dialer	
Extended Networking	
VPN	
DNS/WINS Resolver	

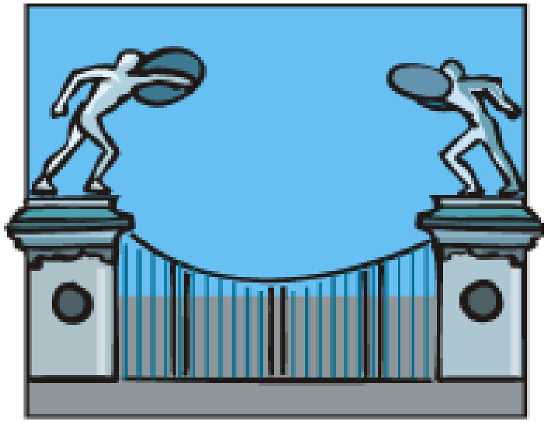
```
DOTNETSRV[bob] - ( bob - Authenticated [NTLM] )
    WinGate Login: Register for everything
XPPR2CPU[SYSTEM]
    WRP Control Session - winlogon.exe
sashex2k
    http://msimg.com/m/8/tab-back_line_tall.gif
    http://msimg.com/m/8/tab-bg_line_on.gif
    http://www.passportimages.com/1033/signin.gif
    http://global.msads.net/ads/1/0000000001_0000000000000
    http://global.msads.net/ads/1/0000000001_0000000000000
    http://msimg.com/m/8/tab-bg_line_off.gif
    http://global.msads.net/ads/6978/0000006978_0000000000
    http://msimg.com/m/8/tab-back_line.gif
    http://msimg.com/m/8/btn_pers_tile.gif
    http://msimg.com/m/8/hs1.jpg
    http://msimg.com/m/8/hs2.jpg
    http://msimg.com/m/8/bullet-black.gif
    http://msimg.com/m/8/bullet-add.gif
```

UserGate Proxy Server

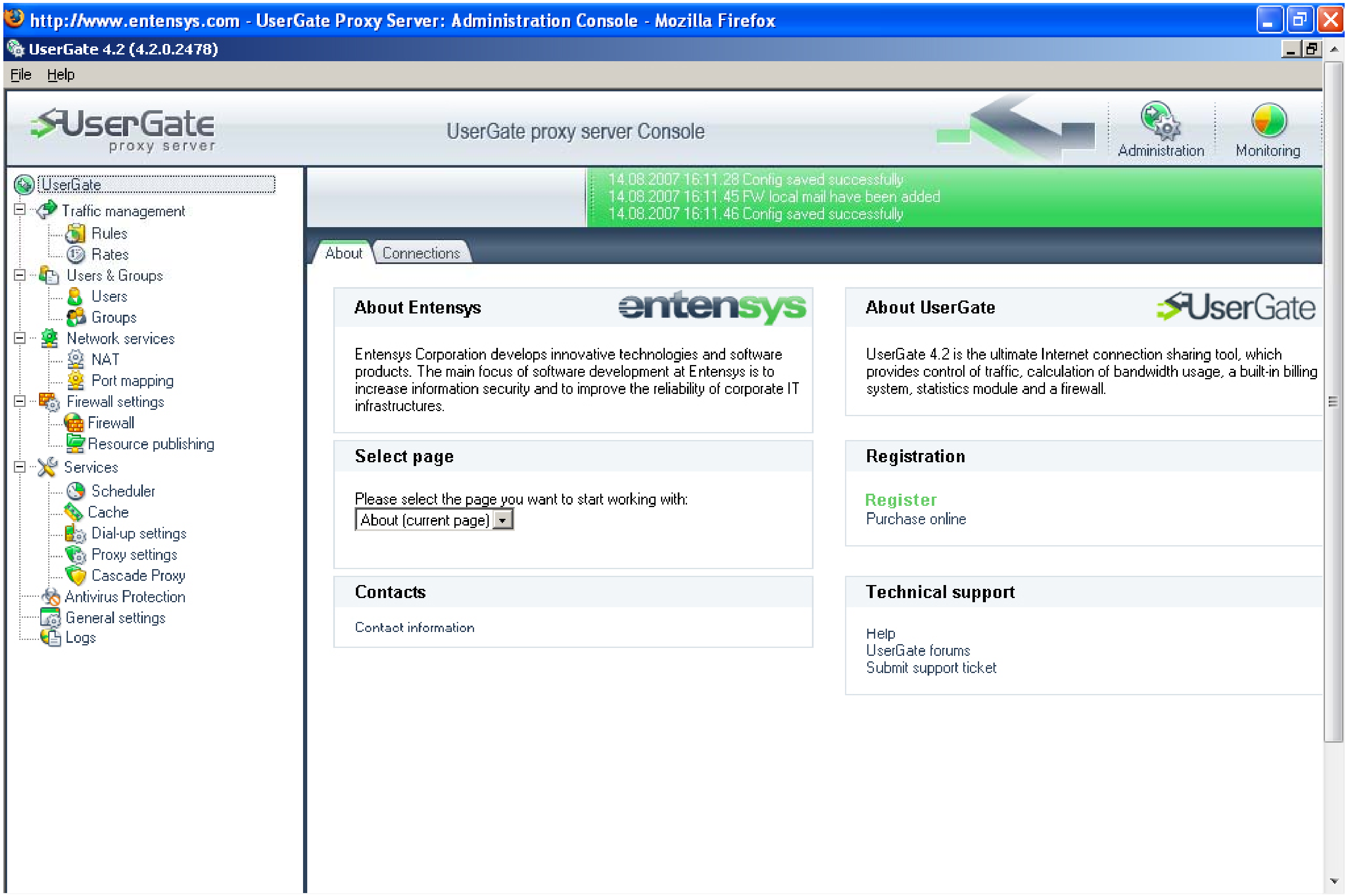
UserGate Proxy and Internet security server is a complex and multifunctional software solution that can be used to connect your network to the Internet

Features:

- Internet Connection Sharing (ICS)
- Internet Traffic Analysis
- User-specific access management
- Administration, alerts and statistics
- Internet Security
- Antivirus Gateway Protection
- General Information
- Release history



UserGate Proxy Server: Screenshot



```
14.08.2007 16:11:28 Config saved successfully
14.08.2007 16:11:45 FW local mail have been added
14.08.2007 16:11:46 Config saved successfully
```

About Entensys

Entensys Corporation develops innovative technologies and software products. The main focus of software development at Entensys is to increase information security and to improve the reliability of corporate IT infrastructures.

About UserGate

UserGate 4.2 is the ultimate Internet connection sharing tool, which provides control of traffic, calculation of bandwidth usage, a built-in billing system, statistics module and a firewall.

Select page

Please select the page you want to start working with:

About (current page)

Registration

Register

Purchase online

Contacts

Contact information

Technical support

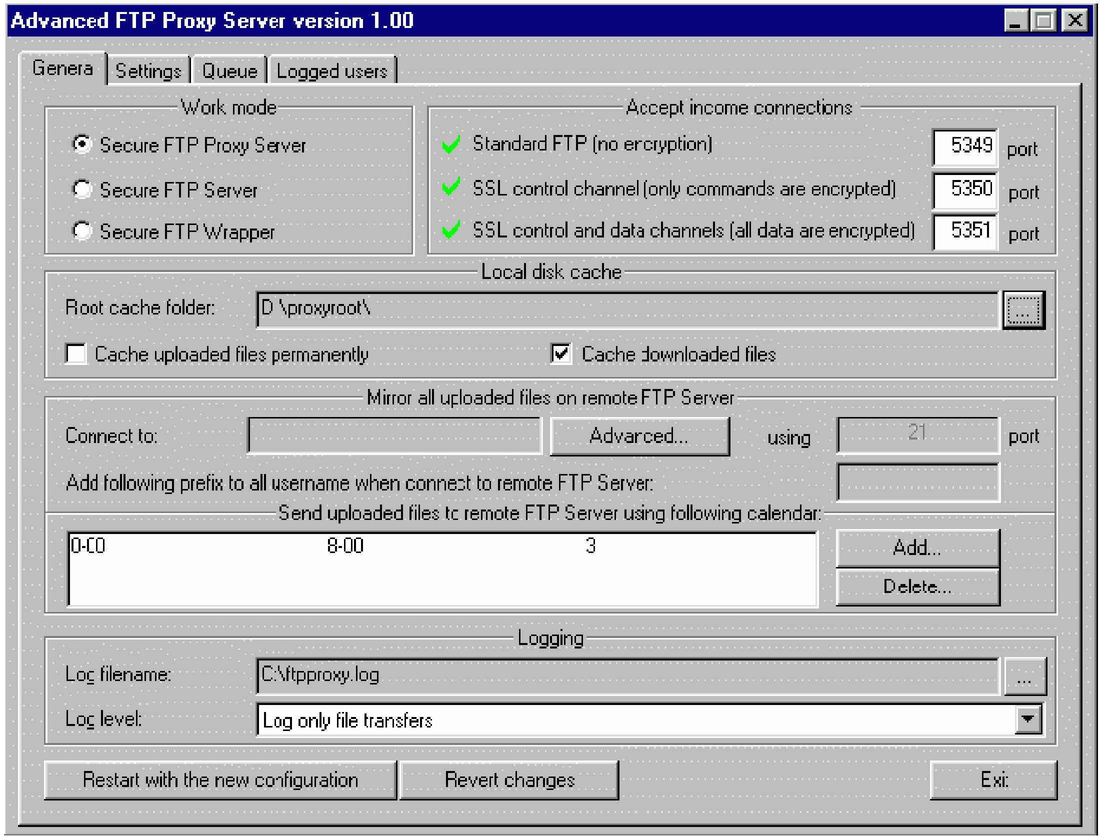
Help

UserGate forums

Submit support ticket

Advanced FTP Proxy Server

Advanced FTP Proxy Server adds encryption and file caching to FTP Server



Advanced FTP Proxy Server version 1.00

Work mode
- ● Secure FTP Proxy Server
- ○ Secure FTP Server
- ○ Secure FTP Wrapper

Accept income connections
- ✓ Standard FTP (no encryption) 5349 port
- ✓ SSL control channel (only commands are encrypted) 5350 port
- ✓ SSL control and data channels (all data are encrypted) 5351 port

Local disk cache

Root cache folder: D \proxyroot\

□ Cache uploaded files permanently ☑ Cache downloaded files

Mirror all uploaded files on remote FTP Server

Connect to: using 21 port

Add following prefix to all username when connect to remote FTP Server:

Send uploaded files tc remote FTP Server using following calendar:

0-00 8-00 3

Logging

Log filename: C:\ftpproxy.log

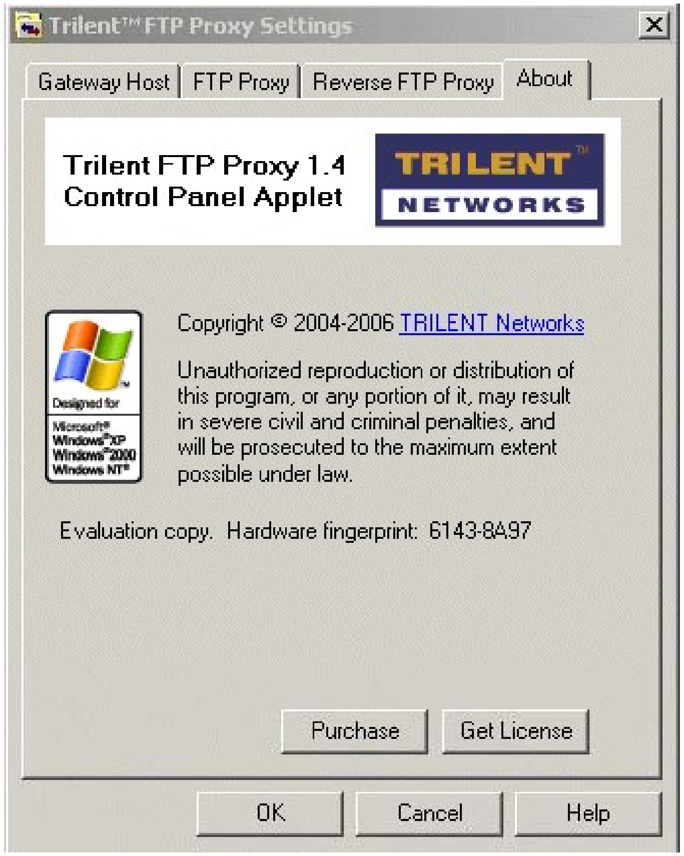
Log level: Log only file transfers

Trilent FTP Proxy

The Trilent FTP Proxy is an application-level proxy that performs smart inspection of the FTP protocol, which enables it to block many Internet threats

Features:

- Sharing Internet Connection
- Reverse Proxying
- Unattended Operation
- Standards Compliance
- Security



Trilent FTP Proxy 1.4
Control Panel Applet

Copyright © 2004-2006 TRILENT Networks

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Evaluation copy. Hardware fingerprint: 6143-8A97

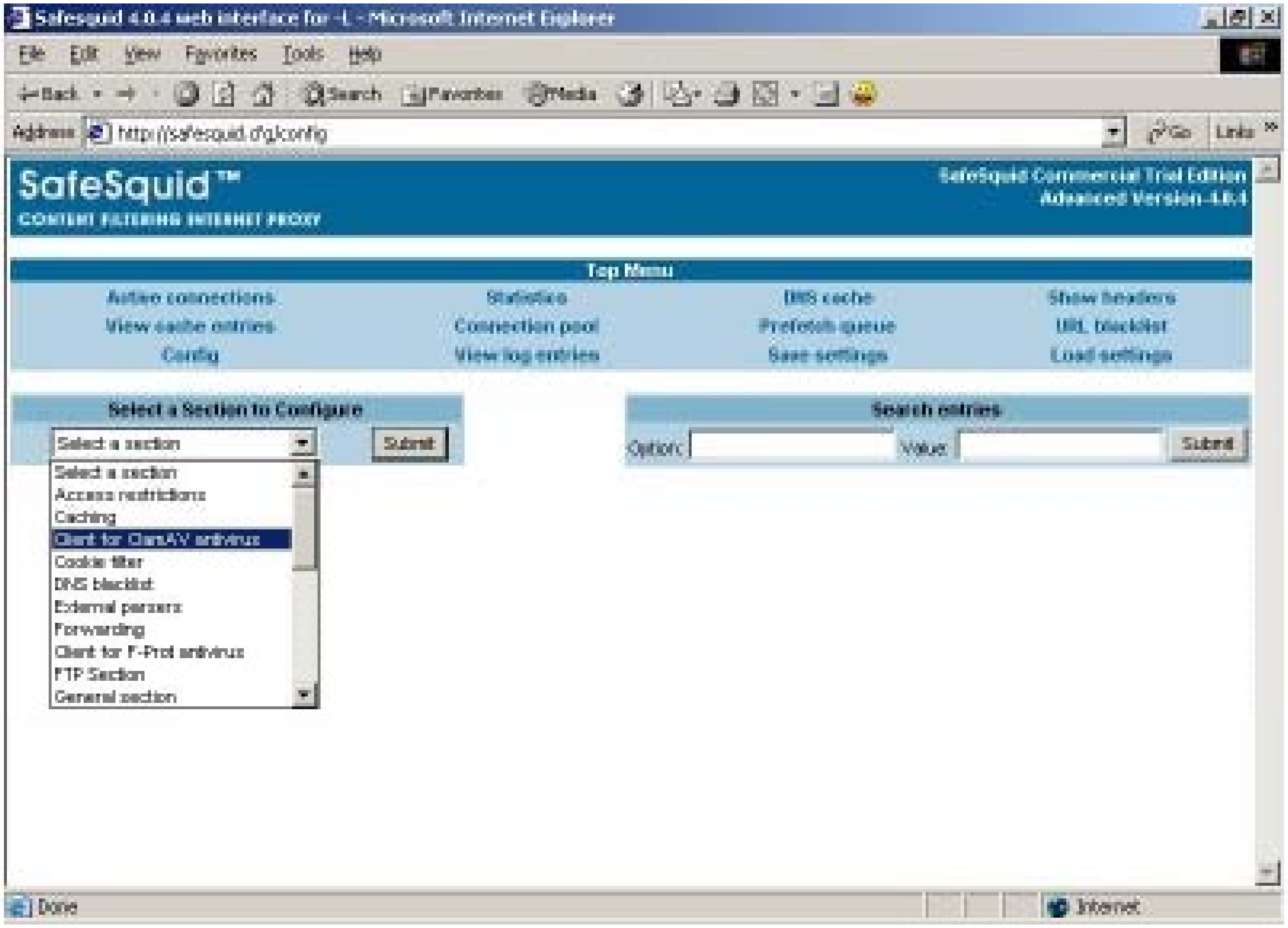
SafeSquid

SafeSquid delivers the essential goals of a Content Filtering Internet Proxy - Total Access Control & Total Content Control

Features:

- Profiled Internet Access
- User Authentication
- Application QoS and Bandwidth Limits
- Caching and Pre-fetching
- Connectivity for Third-party software & services
- Enterprise Wide Management
- Re-Programmable Content Filtering
- Redundant level Content Security
- Customisable Log Reports
- Programmable Custom Templates

SafeSquid: Screenshot



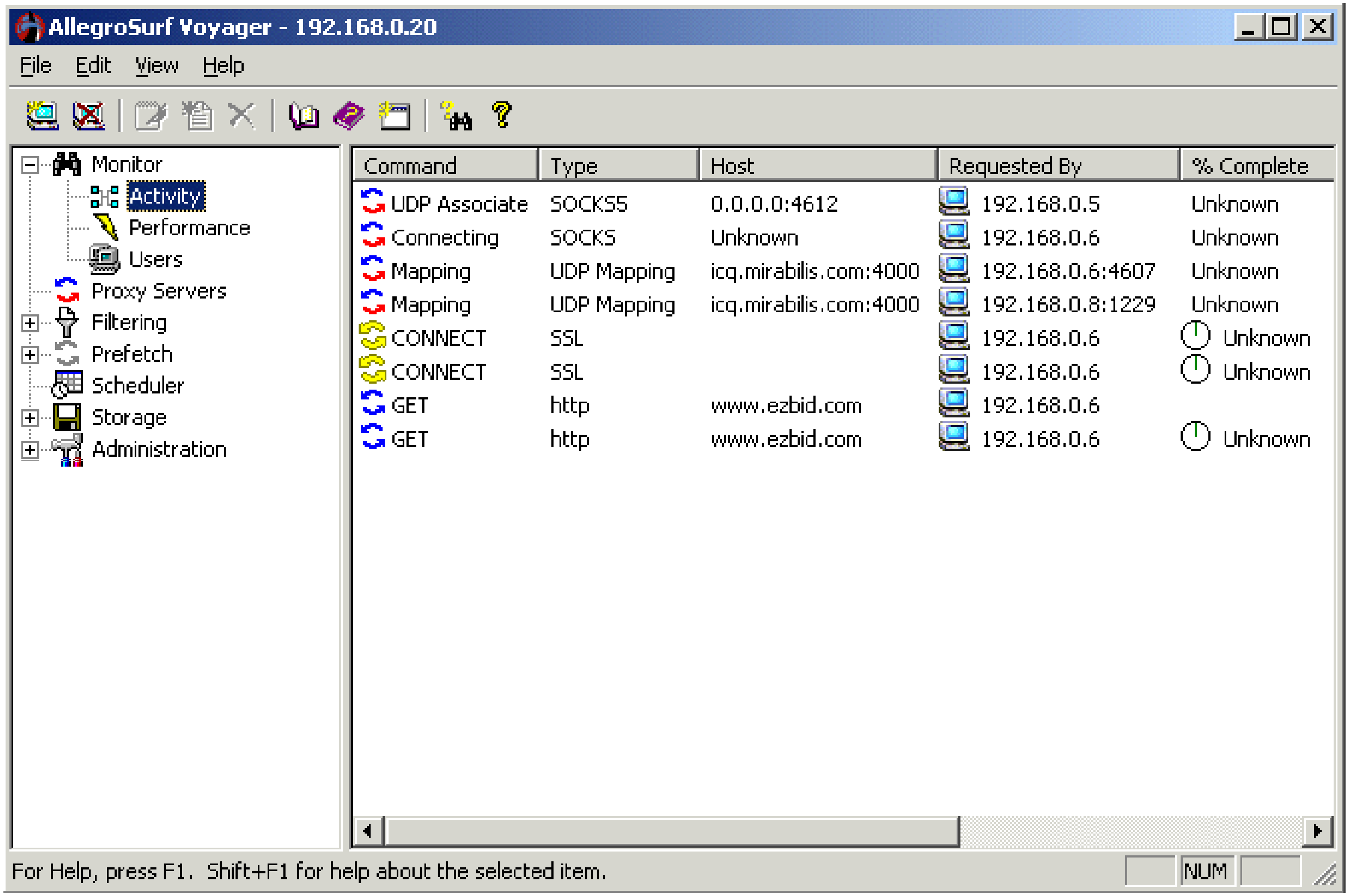
AllegroSurf

AllegroSurf is a web accelerating, content filtering, proxy server

It allows users to share a single Internet connection with multiple computers on a LAN, while protecting users from unwanted content and increasing overall Internet speed

It runs in the background to share Internet connection with the rest of the network

AllegroSurf: Screenshot



Command	Type	Host	Requested By	% Complete
UDP Associate	SOCKS5	0.0.0.0:4612	192.168.0.5	Unknown
Connecting	SOCKS	Unknown	192.168.0.6	Unknown
Mapping	UDP Mapping	icq.mirabilis.com:4000	192.168.0.6:4607	Unknown
Mapping	UDP Mapping	icq.mirabilis.com:4000	192.168.0.8:1229	Unknown
CONNECT	SSL		192.168.0.6	Unknown
CONNECT	SSL		192.168.0.6	Unknown
GET	http	www.ezbid.com	192.168.0.6	
GET	http	www.ezbid.com	192.168.0.6	Unknown

For Help, press F1. Shift+F1 for help about the selected item.

ezProxy

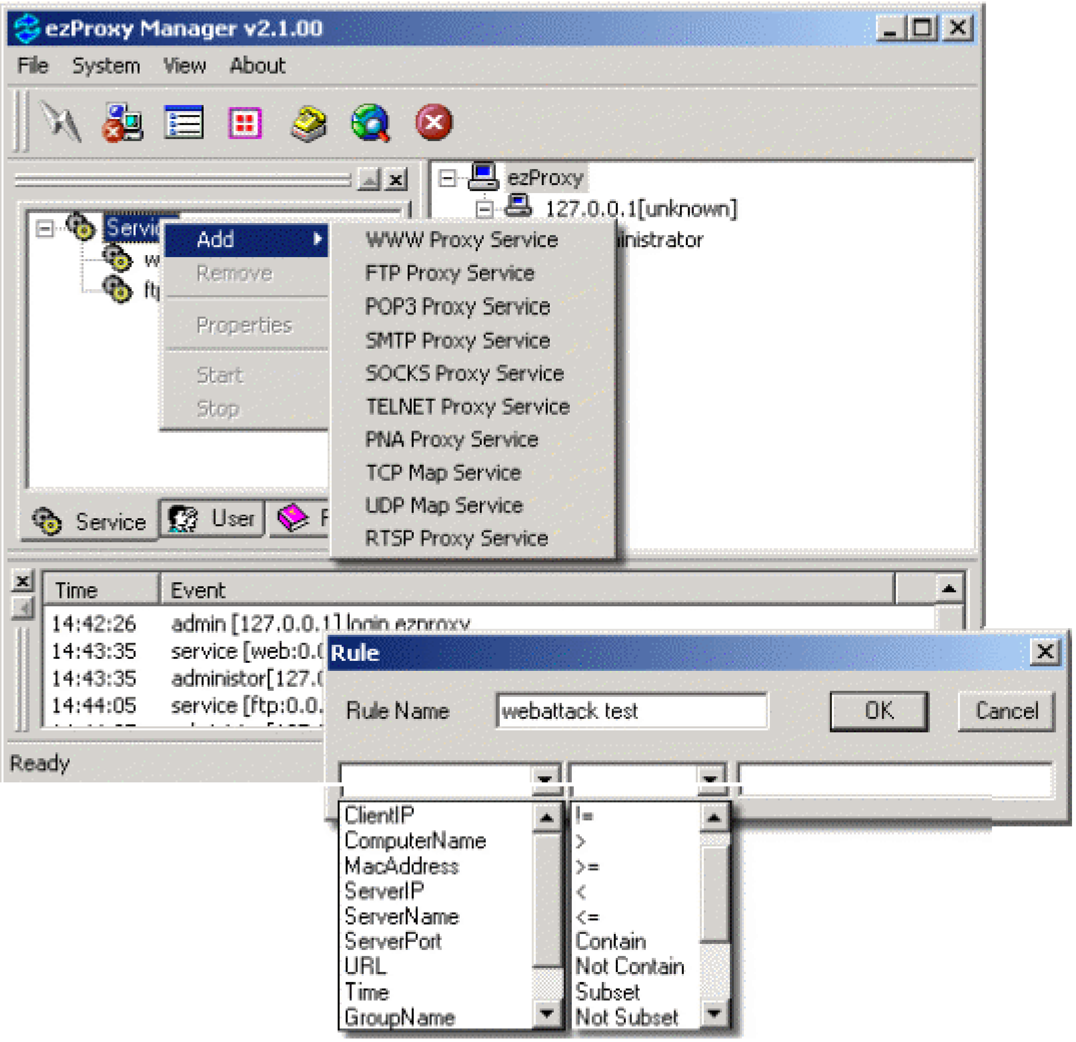
ezProxy allows an entire network to share a single Internet account simultaneously

It protects valuable information on the network with the integrated proxy server/firewall

Users can specify rules for all users or define custom rules and restrictions for individual users

Rules can be saved as policies and applied as needed

ezProxy: Screenshot



```
Time      Event
14:42:26  admin [127.0.0.1] login ezproxy
14:43:35  service [web:0.0
14:43:35  administor[127.0
14:44:05  service [ftp:0.0.
```

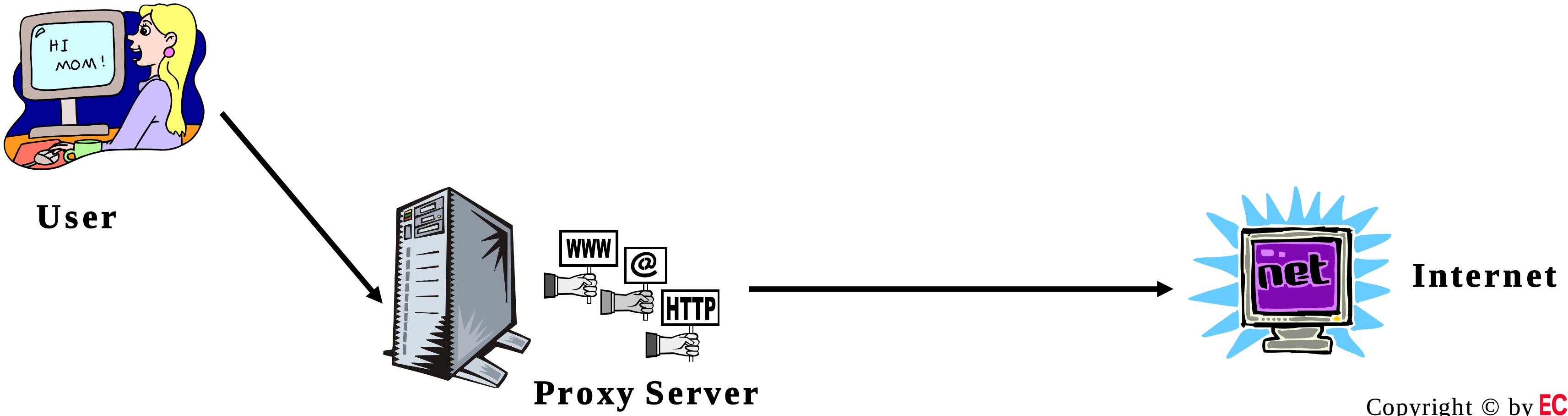
Rule Name: webattack test

Proxy Workbench

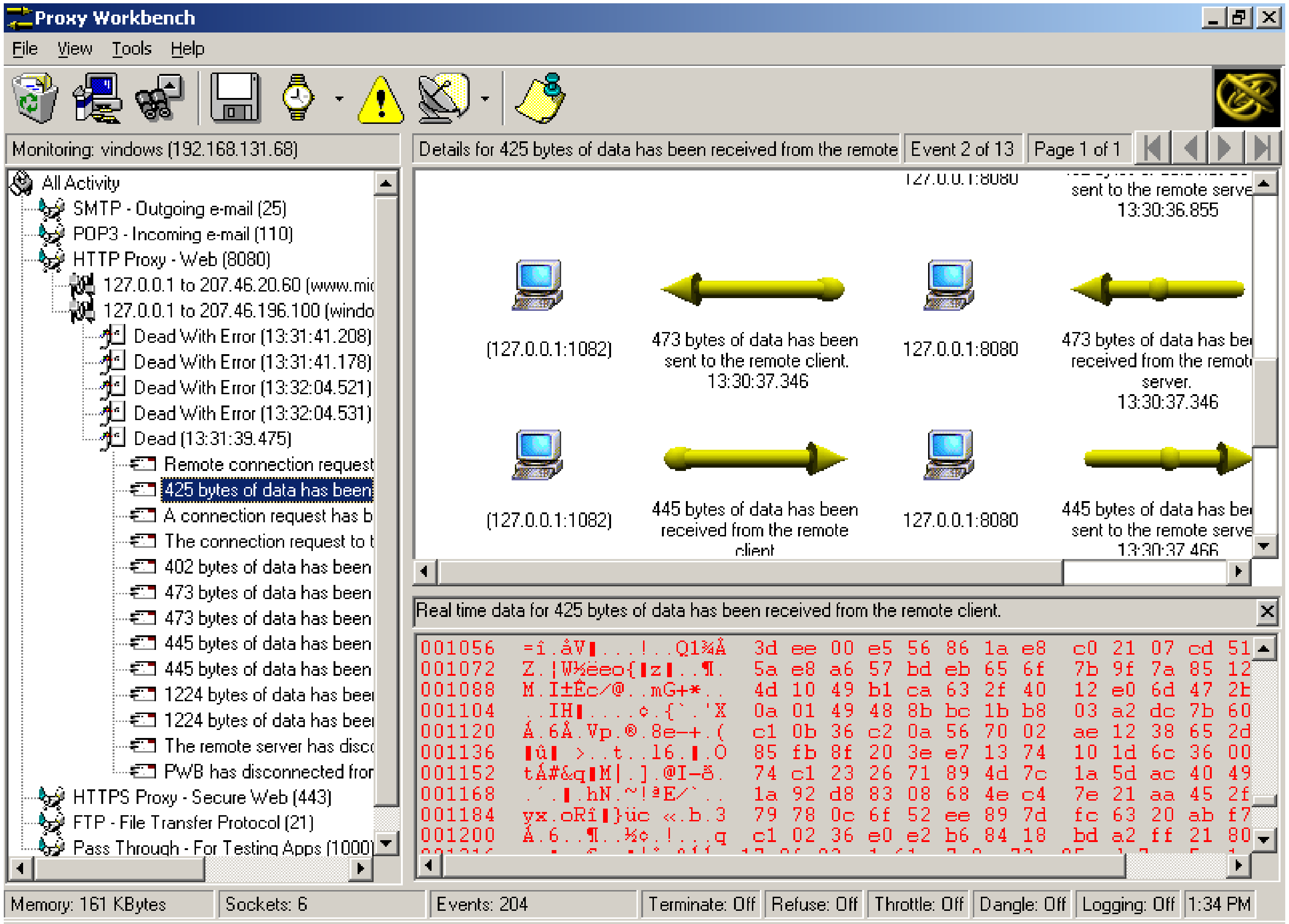
Proxy Workbench is a small proxy server which sits inside the network and monitors connection

Configuration:

- Install Proxy Workbench
- Configure the clients to use this proxy IP to connect to port 8080



Proxy Workbench: Screenshot



Monitoring: vindows (192.168.131.68)

Details for 425 bytes of data has been received from the remote

Event 2 of 13

Page 1 of 1

- All Activity
  - SMTP - Outgoing e-mail (25)
  - POP3 - Incoming e-mail (110)
  - HTTP Proxy - Web (8080)
    - 127.0.0.1 to 207.46.20.60 (www.mic
    - 127.0.0.1 to 207.46.196.100 (windo
      - Dead With Error (13:31:41.208)
      - Dead With Error (13:31:41.178)
      - Dead With Error (13:32:04.521)
      - Dead With Error (13:32:04.531)
      - Dead (13:31:39.475)
        - Remote connection request
        - 425 bytes of data has been
        - A connection request has b
        - The connection request to t
        - 402 bytes of data has been
        - 473 bytes of data has been
        - 473 bytes of data has been
        - 445 bytes of data has been
        - 445 bytes of data has been
        - 1224 bytes of data has beer
        - 1224 bytes of data has beer
        - The remote server has disco
        - PWB has disconnected fror
  - HTTPS Proxy - Secure Web (443)
  - FTP - File Transfer Protocol (21)
  - Pass Through - For Testing Apps (1000)

127.0.0.1:8080

sent to the remote serve
13:30:36.855

(127.0.0.1:1082)

473 bytes of data has been sent to the remote client.
13:30:37.346

127.0.0.1:8080

473 bytes of data has bei received from the remot server.
13:30:37.346

(127.0.0.1:1082)

445 bytes of data has been received from the remote client

127.0.0.1:8080

445 bytes of data has bei sent to the remote serve
13:30:37.466

Real time data for 425 bytes of data has been received from the remote client.

```
001056   =î.åV▌...!..Q1¾Å   3d ee 00 e5 56 86 1a e8  c0 21 07 cd 51
001072   Z.¦W½ëeo{▌z▌..¶.   5a e8 a6 57 bd eb 65 6f  7b 9f 7a 85 12
001088   M.I±Êc/@..mG+*..   4d 10 49 b1 ca 63 2f 40  12 e0 6d 47 2b
001104   ..IH▌....¢.{`.'X   0a 01 49 48 8b bc 1b b8  03 a2 dc 7b 60
001120   Á.6Â.Vp.®.8e-+.(   c1 0b 36 c2 0a 56 70 02  ae 12 38 65 2d
001136   ▌û▌ >..t..16.▌.O   85 fb 8f 20 3e e7 13 74  10 1d 6c 36 00
001152   tÁ#&q▌M|.].@I-ð.   74 c1 23 26 71 89 4d 7c  1a 5d ac 40 49
001168   .´.▌.hN.~!ªE/`..   1a 92 d8 83 08 68 4e c4  7e 21 aa 45 2f
001184   yx.oRî▌}üc «.b.3   79 78 0c 6f 52 ee 89 7d  fc 63 20 ab f7
001200   Á.6..¶..½¢.!...q   c1 02 36 e0 e2 b6 84 18  bd a2 ff 21 80
```

Memory: 161 KBytes | Sockets: 6 | Events: 204 | Terminate: Off | Refuse: Off | Throttle: Off | Dangle: Off | Logging: Off | 1:34 PM

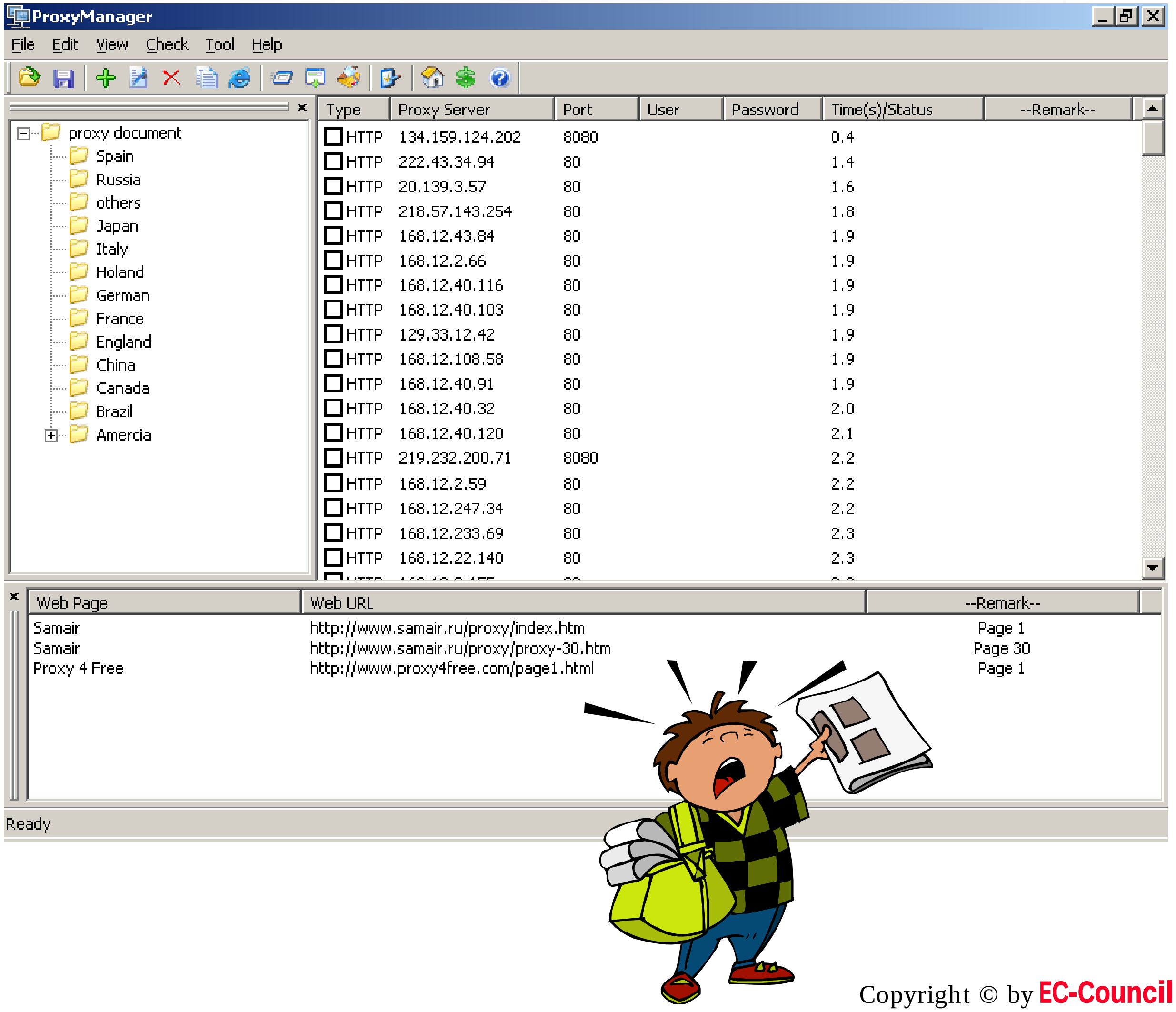
EC-Council

ProxyManager Tool

ProxyManager connects to the Internet and downloads lists of proxy servers from various websites

You will have thousands of proxy server IP addresses within minutes

Saves time instead of manually visiting individual web sites looking for free proxy servers



Type	Proxy Server	Port	User	Password	Time(s)/Status	--Remark--
□ HTTP	134.159.124.202	8080			0.4	
□ HTTP	222.43.34.94	80			1.4	
□ HTTP	20.139.3.57	80			1.6	
□ HTTP	218.57.143.254	80			1.8	
□ HTTP	168.12.43.84	80			1.9	
□ HTTP	168.12.2.66	80			1.9	
□ HTTP	168.12.40.116	80			1.9	
□ HTTP	168.12.40.103	80			1.9	
□ HTTP	129.33.12.42	80			1.9	
□ HTTP	168.12.108.58	80			1.9	
□ HTTP	168.12.40.91	80			1.9	
□ HTTP	168.12.40.32	80			2.0	
□ HTTP	168.12.40.120	80			2.1	
□ HTTP	219.232.200.71	8080			2.2	
□ HTTP	168.12.2.59	80			2.2	
□ HTTP	168.12.247.34	80			2.2	
□ HTTP	168.12.233.69	80			2.3	
□ HTTP	168.12.22.140	80			2.3	

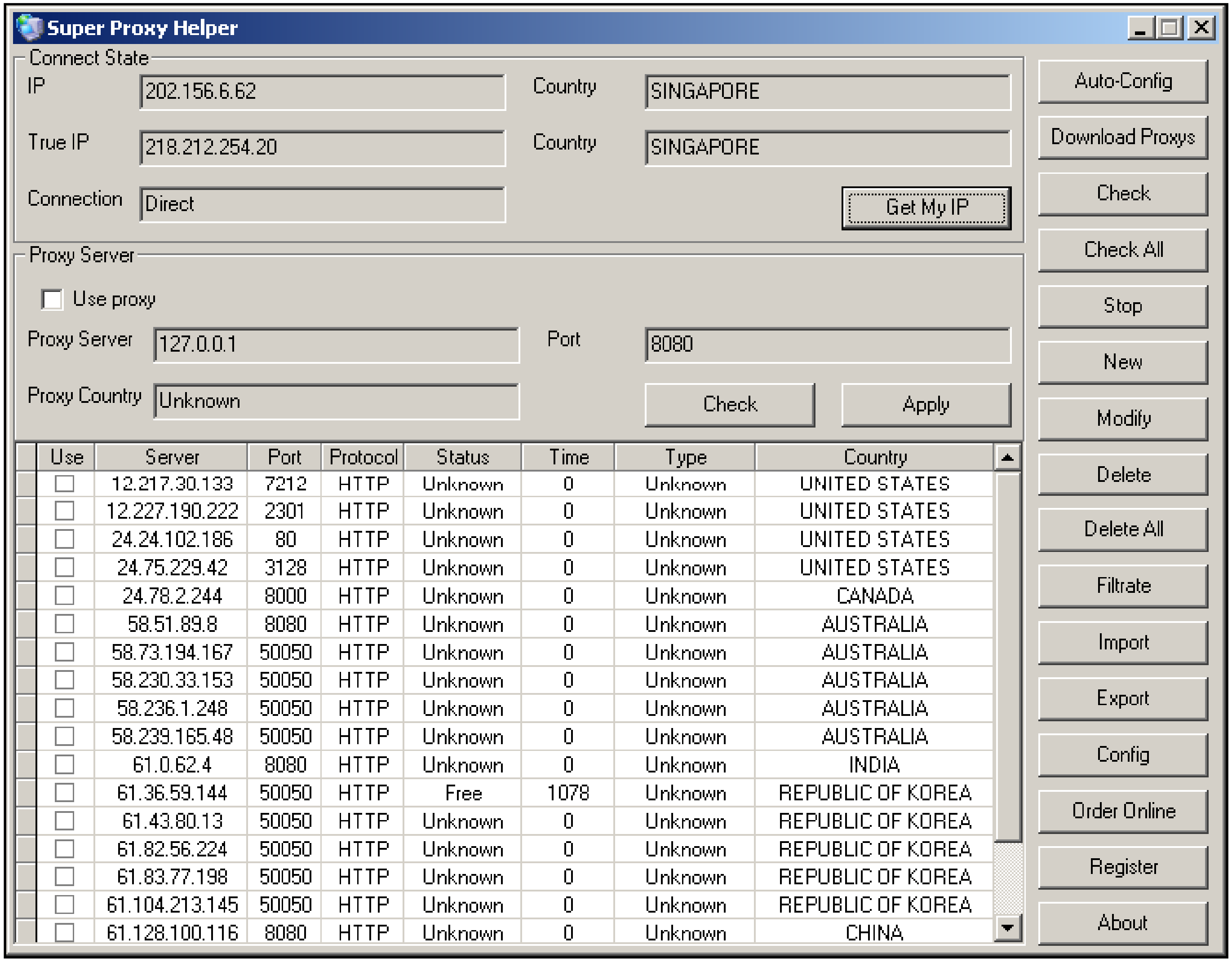
Web Page	Web URL	--Remark--
Samair	http://www.samair.ru/proxy/index.htm	Page 1
Samair	http://www.samair.ru/proxy/proxy-30.htm	Page 30
Proxy 4 Free	http://www.proxy4free.com/page1.html	Page 1

Super Proxy Helper Tool

Super Proxy Helper will help you to:

- Find anonymous, free, or fastest proxy
- Check proxy status response time within a country
- Determine Proxy type (Transparent, Anonymous, or High anonymity)
- Import export proxy
- Download proxy lists from the web

Super Proxy Helper Tool: Screenshot



Connect State

IP	202.156.6.62	Country	SINGAPORE
True IP	218.212.254.20	Country	SINGAPORE
Connection	Direct		

Proxy Server

□ Use proxy

Proxy Server	127.0.0.1	Port	8080
Proxy Country	Unknown		

Use	Server	Port	Protocol	Status	Time	Type	Country
□	12.217.30.133	7212	HTTP	Unknown	0	Unknown	UNITED STATES
□	12.227.190.222	2301	HTTP	Unknown	0	Unknown	UNITED STATES
□	24.24.102.186	80	HTTP	Unknown	0	Unknown	UNITED STATES
□	24.75.229.42	3128	HTTP	Unknown	0	Unknown	UNITED STATES
□	24.78.2.244	8000	HTTP	Unknown	0	Unknown	CANADA
□	58.51.89.8	8080	HTTP	Unknown	0	Unknown	AUSTRALIA
□	58.73.194.167	50050	HTTP	Unknown	0	Unknown	AUSTRALIA
□	58.230.33.153	50050	HTTP	Unknown	0	Unknown	AUSTRALIA
□	58.236.1.248	50050	HTTP	Unknown	0	Unknown	AUSTRALIA
□	58.239.165.48	50050	HTTP	Unknown	0	Unknown	AUSTRALIA
□	61.0.62.4	8080	HTTP	Unknown	0	Unknown	INDIA
□	61.36.59.144	50050	HTTP	Free	1078	Unknown	REPUBLIC OF KOREA
□	61.43.80.13	50050	HTTP	Unknown	0	Unknown	REPUBLIC OF KOREA
□	61.82.56.224	50050	HTTP	Unknown	0	Unknown	REPUBLIC OF KOREA
□	61.83.77.198	50050	HTTP	Unknown	0	Unknown	REPUBLIC OF KOREA
□	61.104.213.145	50050	HTTP	Unknown	0	Unknown	REPUBLIC OF KOREA
□	61.128.100.116	8080	HTTP	Unknown	0	Unknown	CHINA

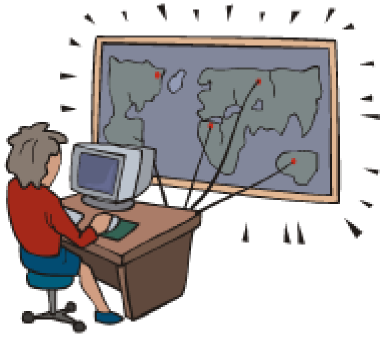
MultiProxy

What if your Firewall is blocking you from various proxy servers and anonymizers?

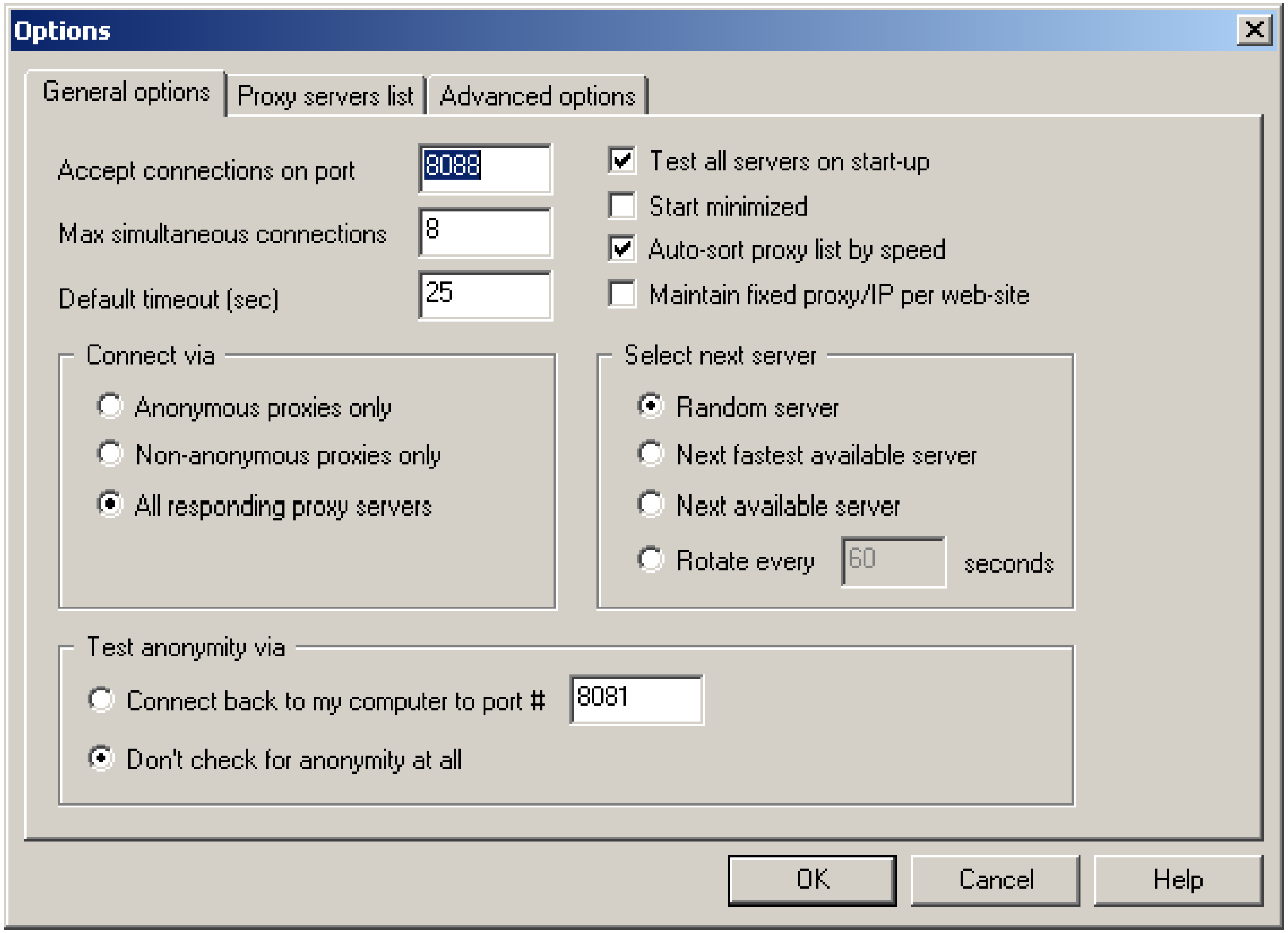
MultiProxy uses different proxies every time you visit the Internet

Adds thousands of proxies to the list and your Firewall does not see a pattern in your traffic

This tool can make it difficult to trace



MultiProxy: Screenshot



Options

Accept connections on port: 8088

Max simultaneous connections: 8

Default timeout (sec): 25

☑ Test all servers on start-up

□ Start minimized

☑ Auto-sort proxy list by speed

□ Maintain fixed proxy/IP per web-site

Connect via

○ Anonymous proxies only

○ Non-anonymous proxies only

● All responding proxy servers

Select next server

● Random server

○ Next fastest available server

○ Next available server

○ Rotate every 60 seconds

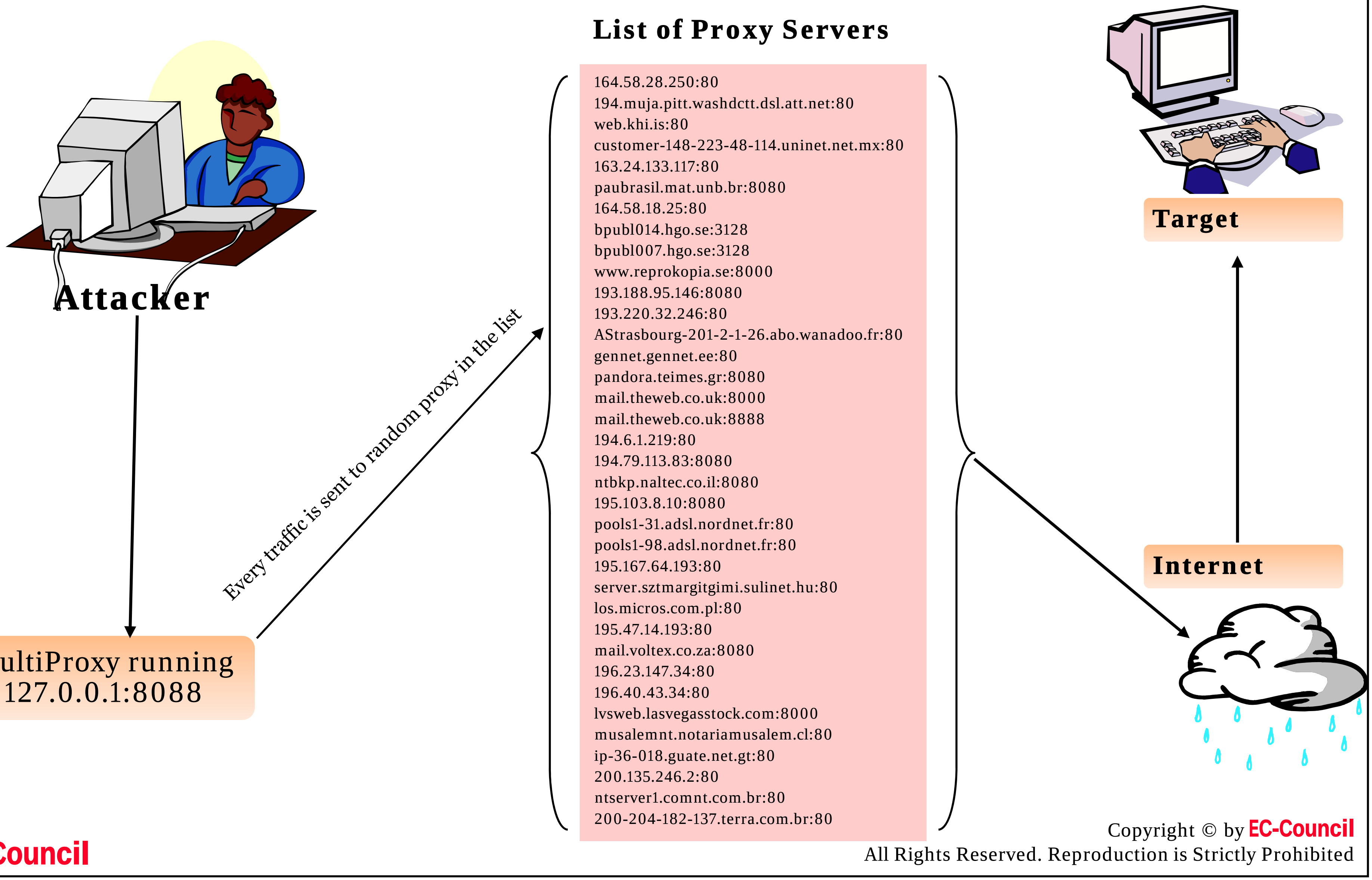
Test anonymity via

○ Connect back to my computer to port # 8081

● Don't check for anonymity at all

EC-Council

How Does MultiProxy Work



Attacker

MultiProxy running at 127.0.0.1:8088

Every traffic is sent to random proxy in the list

List of Proxy Servers

164.58.28.250:80
194.muja.pitt.washdctt.dsl.att.net:80
web.khi.is:80
customer-148-223-48-114.uninet.net.mx:80
163.24.133.117:80
paubrasil.mat.unb.br:8080
164.58.18.25:80
bpubl014.hgo.se:3128
bpubl007.hgo.se:3128
www.reprokopia.se:8000
193.188.95.146:8080
193.220.32.246:80
AStrasbourg-201-2-1-26.abo.wanadoo.fr:80
gennet.gennet.ee:80
pandora.teimes.gr:8080
mail.theweb.co.uk:8000
mail.theweb.co.uk:8888
194.6.1.219:80
194.79.113.83:8080
ntbkp.naltec.co.il:8080
195.103.8.10:8080
pools1-31.adsl.nordnet.fr:80
pools1-98.adsl.nordnet.fr:80
195.167.64.193:80
server.sztmargitgimi.sulinet.hu:80
los.micros.com.pl:80
195.47.14.193:80
mail.voltex.co.za:8080
196.23.147.34:80
196.40.43.34:80
lvsweb.lasvegasstock.com:8000
musalemnt.notariamusalem.cl:80
ip-36-018.guate.net.gt:80
200.135.246.2:80
ntserver1.comnt.com.br:80
200-204-182-137.terra.com.br:80

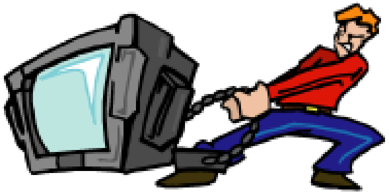
Target

Internet

CEH™
Certified Ethical Hacker

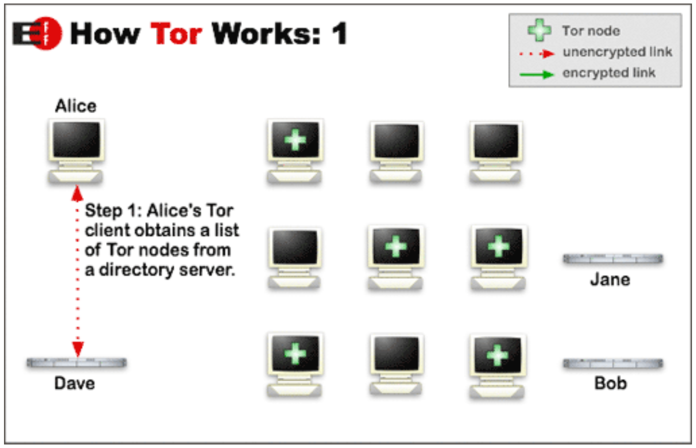
TOR Proxy Chaining Software

- Tor is a network of virtual tunnels connected together and works like a big chained proxy
- It masks the identity of the originating computer from the Internet
- Tor uses random set of servers every time a user visits a site
- A branch of the U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while being deployed in the Middle East
- Law enforcement agencies use Tor for visiting or surveillance of web sites without leaving government IP addresses in their web logs, and for security during sting operations
- Visit http://tor.eff.com



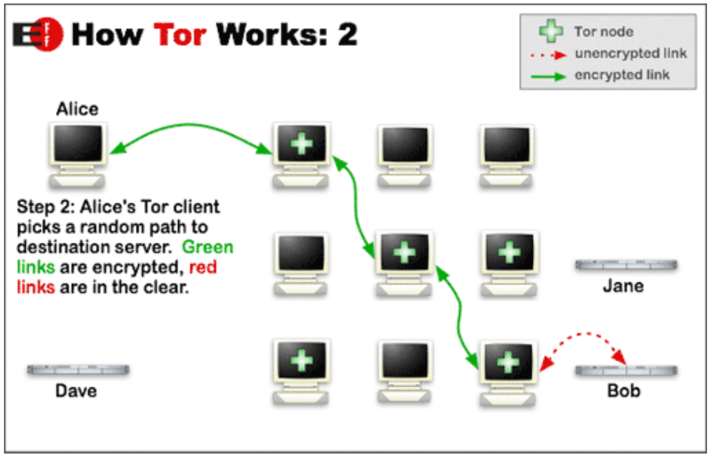
Certified Ethical Hacker

TOR Proxy Chaining Software



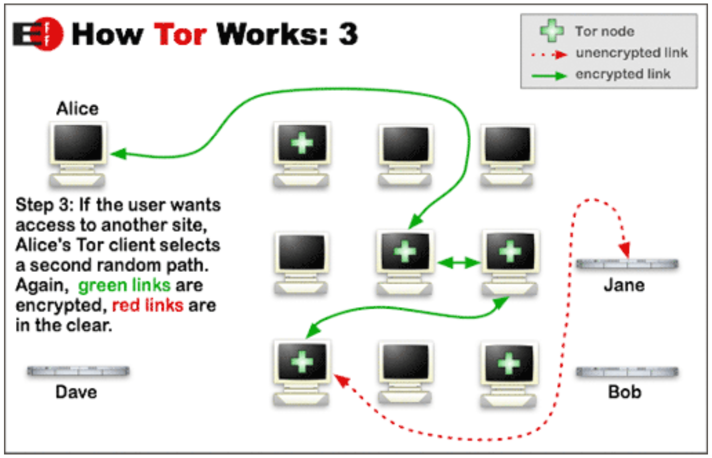
How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.



How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.



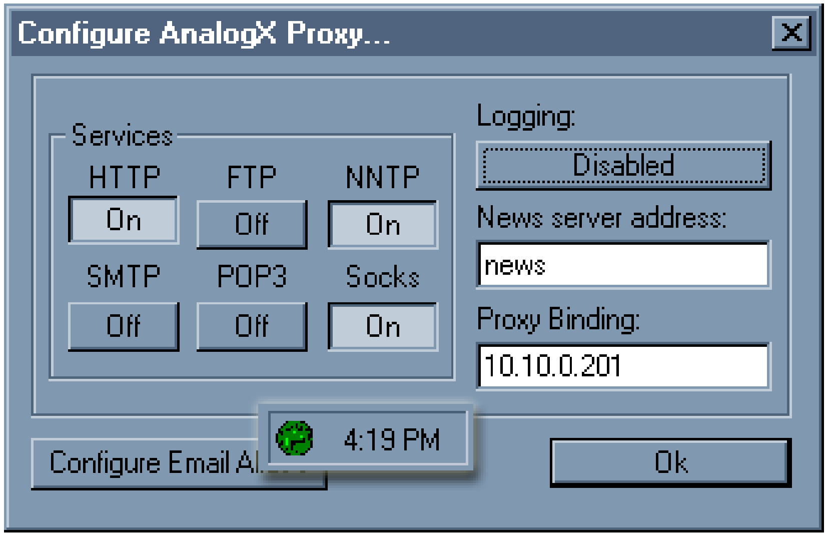
How Tor Works: 3

Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

AnalogX Proxy

AnalogX Proxy is a small and simple server that allows any other machine on your local network to route it's requests through a central machine

Supports HTTP (web), HTTPS (secure web), POP3 (receive mail), SMTP (send mail), NNTP (newsgroups), FTP (file transfer), and Socks4/4a and partial Socks5 (no UDP) protocols



Configure AnalogX Proxy...

Services

HTTP: On

FTP: Off

NNTP: On

SMTP: Off

POP3: Off

Socks: On

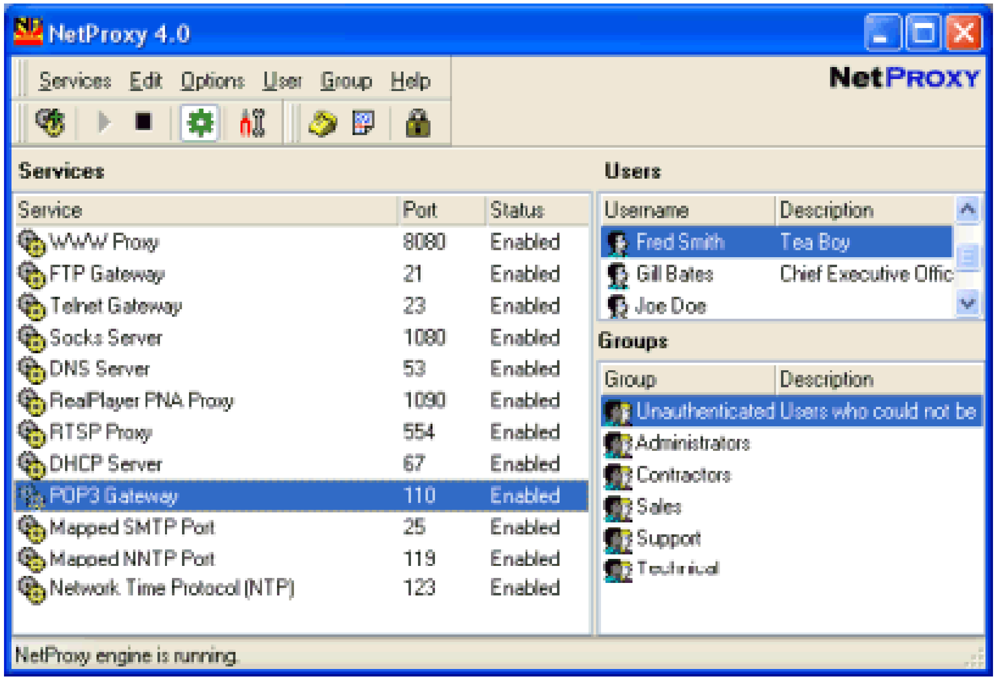
Logging: Disabled

News server address: news

Proxy Binding: 10.10.0.201

NetProxy

NetProxy is a secure, reliable, and highly cost-effective method of providing simultaneous Internet access to multiple network users with only one Internet connection of almost any type



Services

Service	Port	Status
WWW Proxy	8080	Enabled
FTP Gateway	21	Enabled
Telnet Gateway	23	Enabled
Socks Server	1080	Enabled
DNS Server	53	Enabled
RealPlayer PNA Proxy	1090	Enabled
RTSP Proxy	554	Enabled
DHCP Server	67	Enabled
POP3 Gateway	110	Enabled
Mapped SMTP Port	25	Enabled
Mapped NNTP Port	119	Enabled
Network Time Protocol (NTP)	123	Enabled

Users

Username	Description
Fred Smith	Tea Boy
Gill Bates	Chief Executive Offic
Joe Doe	

Groups

Group	Description
Unauthenticated Users who could not be	
Administrators	
Contractors	
Sales	
Support	
Technical	

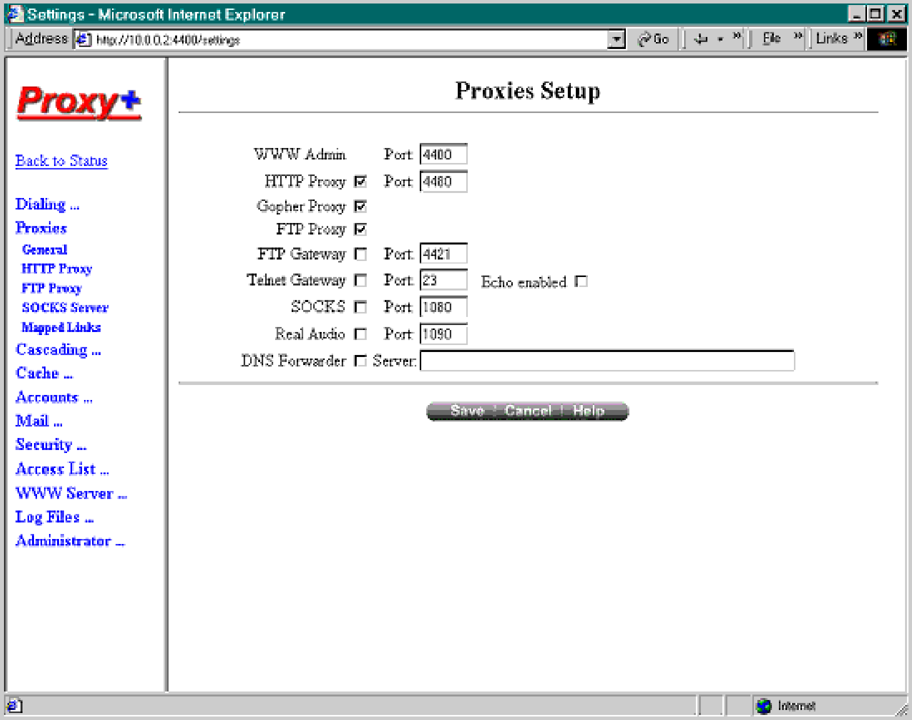
NetProxy engine is running.

Proxy+

Proxy+ works as firewall proxy server and mail server

Features:

- Separates the LAN from the Internet to protect from attacks
- Insecure interfaces (connected to the internet) are detected automatically
- Cache increases speed of data retrieval and enables the use of data even if a connection isn't established
- Sends and receives mail for many Internet mail boxes at one time using the POP3 protocol
- Full SMTP mail server for one or more domains
- Option for leaving messages on POP3 server



http://10.0.0.2:4400/settings

Proxies Setup

WWW Admin Port 4400
HTTP Proxy ☑ Port 4480
Gopher Proxy ☑
FTP Proxy ☑
FTP Gateway □ Port 4421
Telnet Gateway □ Port 23 Echo enabled □
SOCKS □ Port 1080
Real Audio □ Port 1090
DNS Forwarder □ Server:

EC-Council

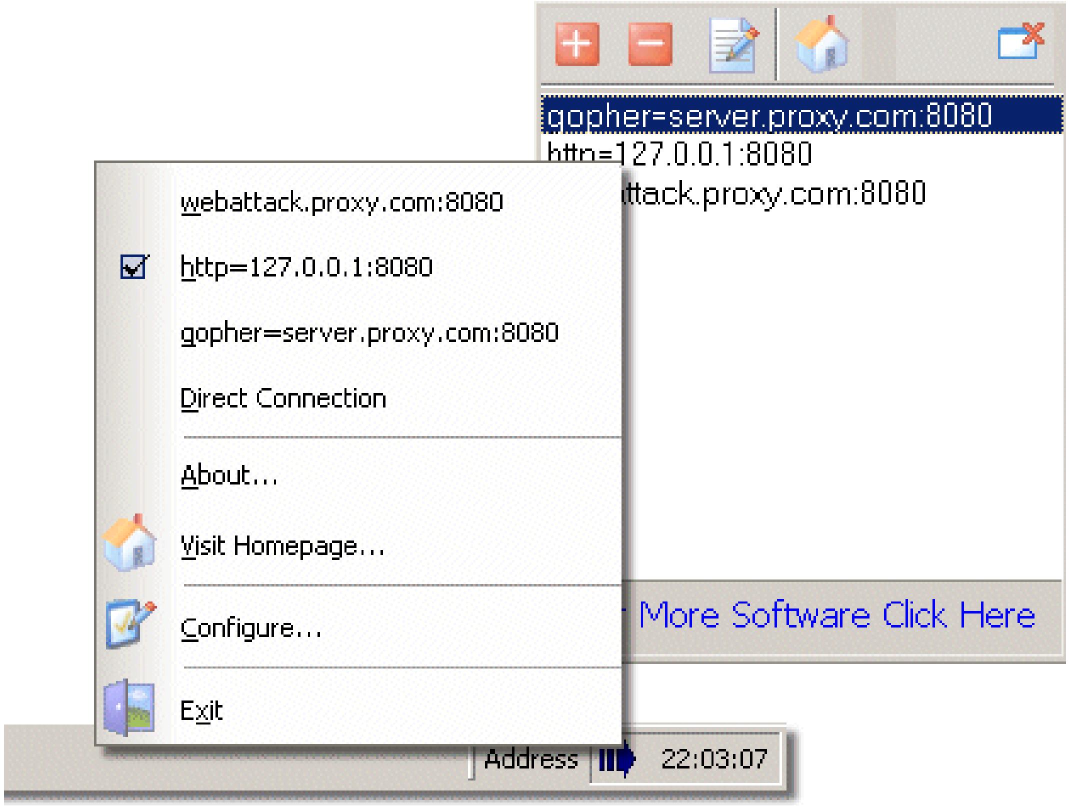
ProxySwitcher Lite

ProxySwitcher Lite is a handy tool to quickly switch between different proxy servers while surfing the Internet

Features:

- Change proxy settings on the fly
- Automatic proxy server switching for anonymous surfing
- Works with Internet Explorer, Firefox, Opera, and others
- Flexible proxy list management
- Proxy server availability testing
- Anonymous proxy server list download

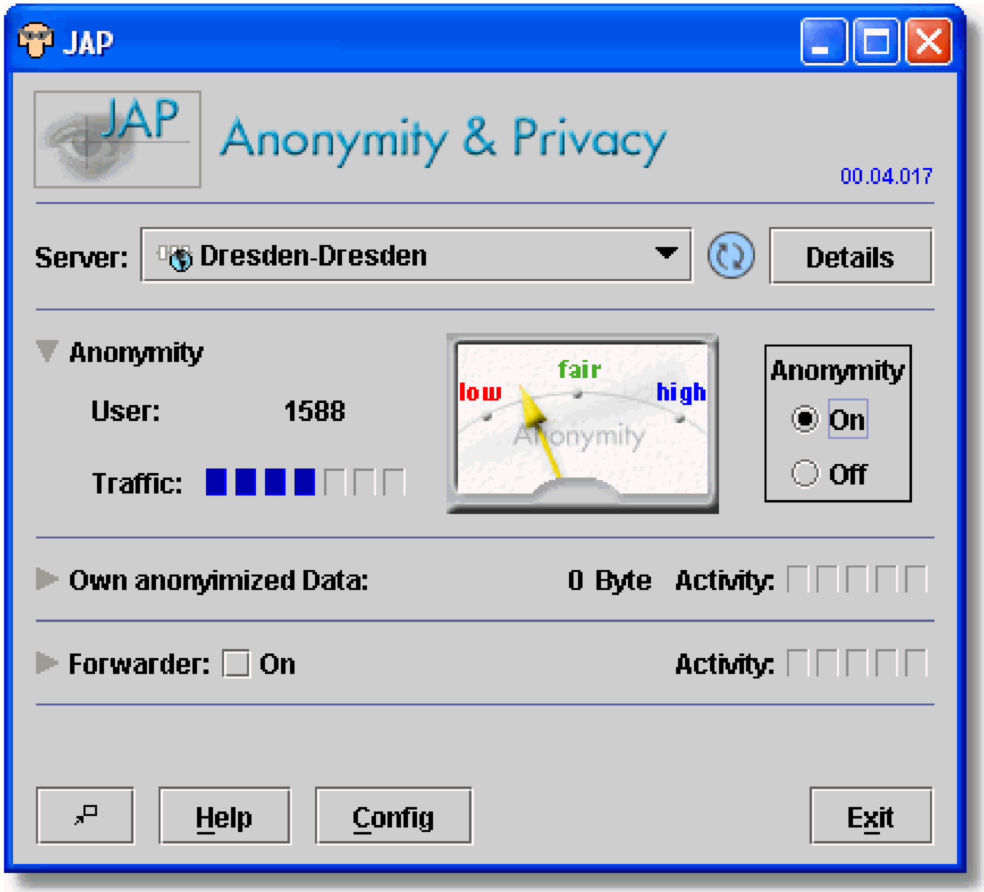
ProxySwitcher Lite: Screenshot



EC-Council

Tool: JAP

JAP enables anonymous web surfing with any browser through the use of integrated proxy services that hide your real IP address



JAP

JAP Anonymity & Privacy 00.04.017

Server: Dresden-Dresden

Anonymity

User: 1588

Traffic: ■■■■□□□

Anonymity ● On ○ Off

Own anonyimized Data: 0 Byte Activity: □□□□□

Forwarder: □ On Activity: □□□□□

Proxomitron

Proxomitron is a flexible HTTP web filtering proxy that enables to filter web content in any browser

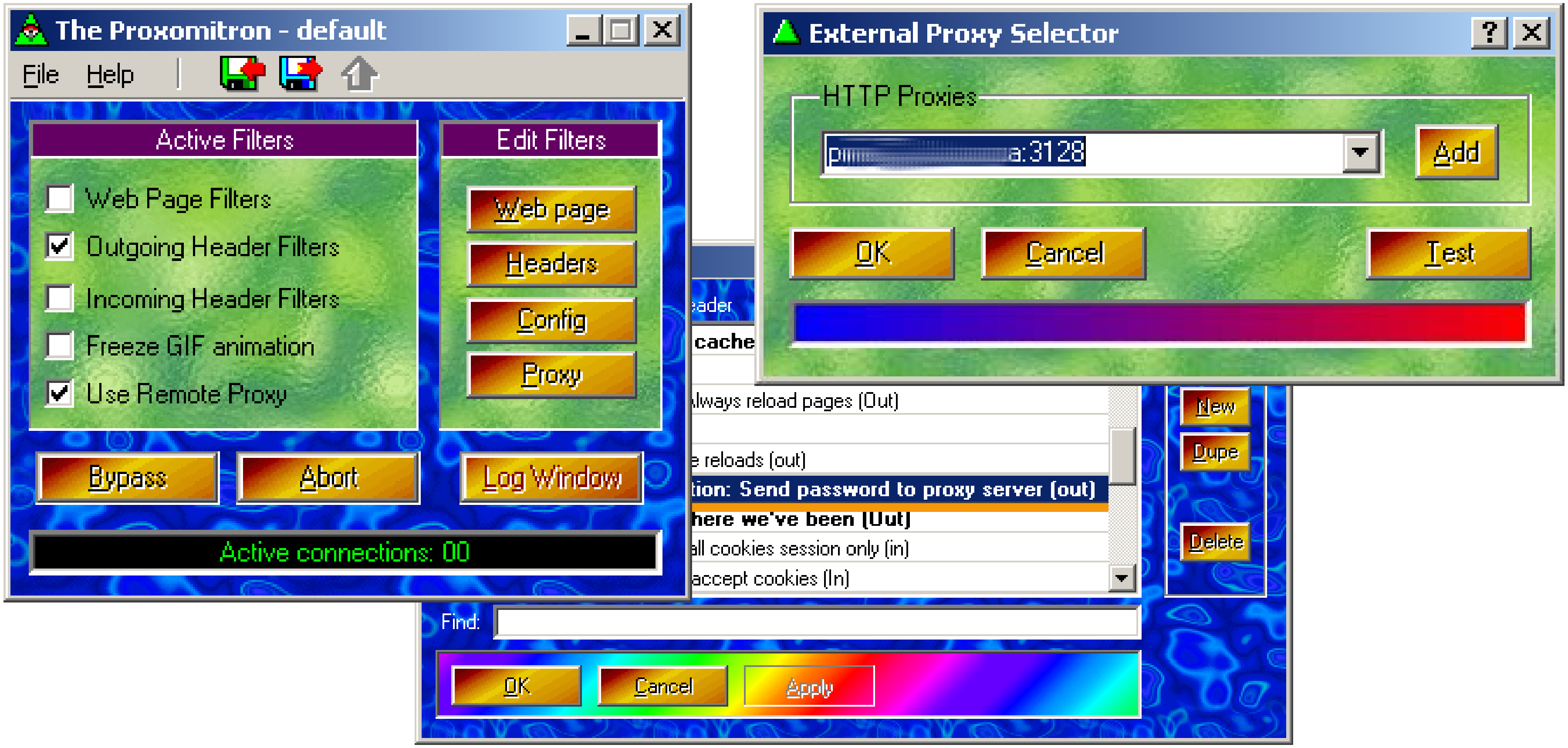
This program runs as a local proxy server and needs to configure browser to use a local host at port 8080 in order to activate filtering

Proxomitron allows you to remove and replace ad banners, Java scripts, off-site images, Flash animations, background images, frames, and many other page elements

HTTP headers can be added, deleted, or changed

Proxomitron filters can be customized and edited as per the requirement

Proxomitron: Screenshot



The Proxomitron - default

File Help

Active Filters

☐ Web Page Filters

☑ Outgoing Header Filters

☐ Incoming Header Filters

☐ Freeze GIF animation

☑ Use Remote Proxy

Active connections: 00

External Proxy Selector

HTTP Proxies

p[redacted]a:3128

eader

cache

lways reload pages (Out)

e reloads (out)

tion: Send password to proxy server (out)

here we've been (Out)

ll cookies session only (in)

accept cookies (In)

Find:

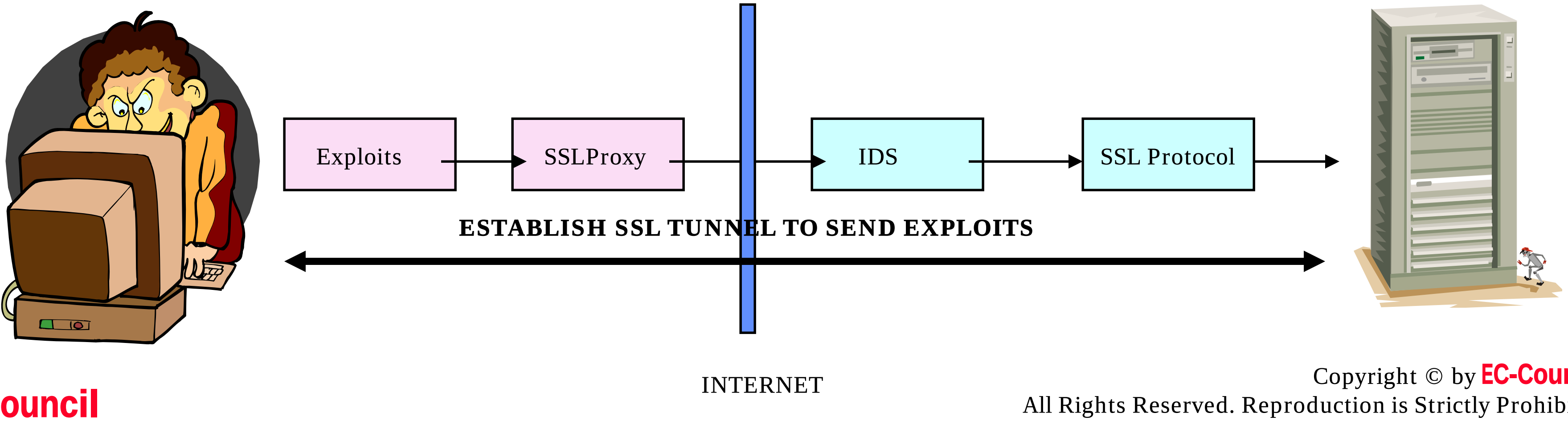
SSL Proxy Tool

SSLproxy is a transparent proxy that can translate between encrypted and unencrypted data transport on socket connections

It also has a non-transparent mode for automatic encryption-detection on netbios

When should I use SSLProxy?

- For example, you want to launch an attack on a remote server which has installed SSL
- The exploits you send will be caught by the IDS and you want to mask this detection
- Run SSLproxy on your machine and tunnel all the exploits through this proxy, which will use SSL to transmit the packets to the remote server blinding the IDS



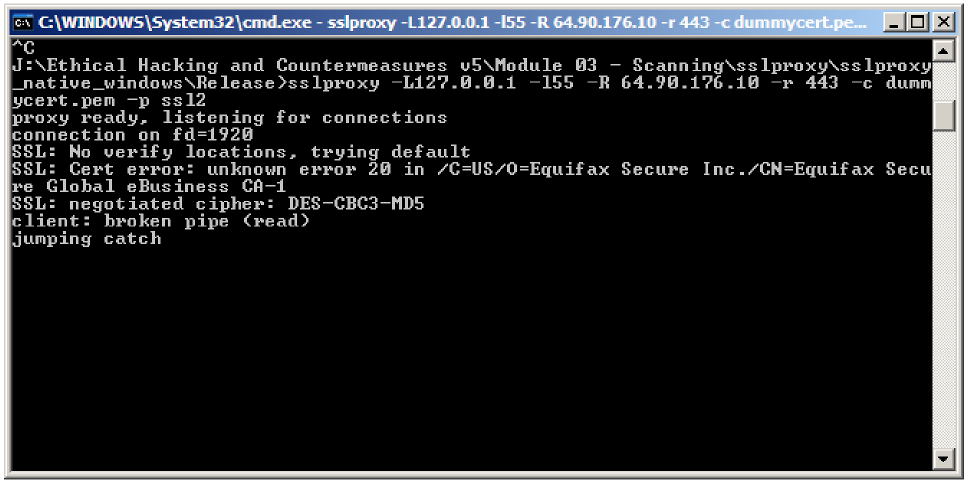
How to Run SSL Proxy

Window 1: Client – Hacker Machine Run:

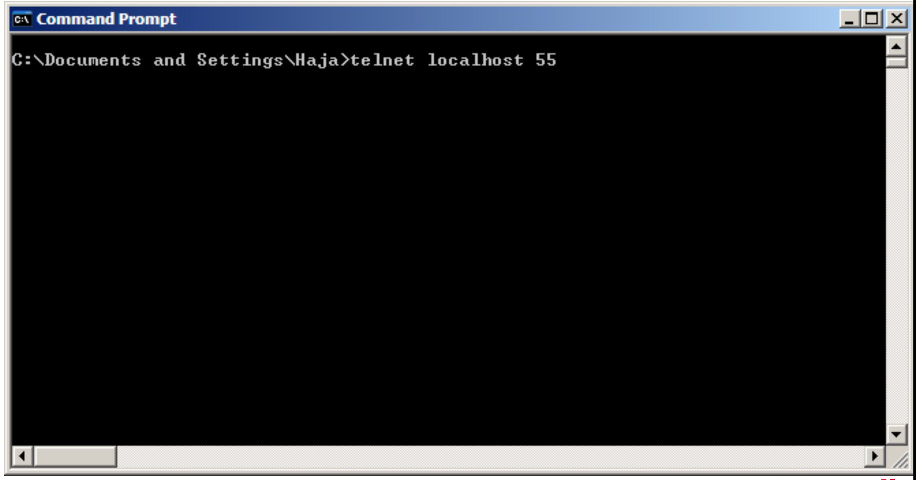
- `sslproxy -L127.0.0.1 -l55 -R <some remote IP> -r 443 -c dummycert.pem -p ssl2`

Window 2: Client - Connect to 12.0.0.1 port 55 and send your exploits

- Example: `telnet 127.0.0.1 55`
- Then type `GET /`


C:\WINDOWS\System32\cmd.exe - sslproxy -L127.0.0.1 -l55 -R 64.90.176.10 -r 443 -c dummycert.pe...

```
^C
J:\Ethical Hacking and Countermeasures v5\Module 03 - Scanning\sslproxy\sslproxy
_native_windows\Release>sslproxy -L127.0.0.1 -l55 -R 64.90.176.10 -r 443 -c dumm
ycert.pem -p ssl2
proxy ready, listening for connections
connection on fd=1920
SSL: No verify locations, trying default
SSL: Cert error: unknown error 20 in /C=US/O=Equifax Secure Inc./CN=Equifax Secu
re Global eBusiness CA-1
SSL: negotiated cipher: DES-CBC3-MD5
client: broken pipe (read)
jumping catch
```



```
C:\Documents and Settings\Haja>telnet localhost 55
```

Summary

Proxy servers act as a connecting link between internal users and external host

Proxy targeted to World Wide web is called Web Proxy

Transparent proxy works on the port 80

Caching proxies stores the copies of recently used and frequently used resources, reducing the upstream bandwidth usage and cost

Copyright 2001 by Randy Glasbergen.
www.glasbergen.com

"Customers aren't impressed by our web site anymore. We need to put the 'gee' back in 'technologee'!"

Copyright 2004 by Randy Glasbergen.
www.glasbergen.com

"Install a patch for the update of the new version. If that doesn't work, install the new version of the update for the patch. If all else fails, install a patch for the new version of the update."